Caveats for Cisco IOS Release 12.0

November 6, 2000

Text Part Number 78-6455-12

Note You can find the most current Cisco IOS documentation on Cisco Connection Online (CCO). These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

This document lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.0, up to and including Release 12.0(14). Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

To improve this document, we would appreciate your comments. If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically at http://www.cisco.com/feedback/ or contact caveats-doc@cisco.com. For more information, see the "Documentation CD-ROM" section on page 159.

How to Use This Document

This document describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" section lists open caveats that apply to the current release and might apply to previous releases.
- The "Resolved Caveats" sections list caveats resolved in a particular release, but open in previous releases.

Within the sections the caveats are sorted by technology in alphabetical order. For example, AppleTalk caveats are listed separately from, and before, IP caveats. The caveats are also sorted alphanumerically by caveat number.

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 1998-2000. Cisco Systems, Inc. All rights reserved.

If You Need More Information

The most up-to-date documentation can be found on the Web through Cisco Connection Online (CCO) and on the latest Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed. For information on CCO, see the "Cisco Connection Online" section on page 158. For more information on the CD-ROM, see the "Documentation CD-ROM" section on page 159.

For more information on caveats and features in Cisco IOS Release 12.0, see the following sources:

- *Internetworking Terms and Acronyms*—The Internetworking Terms and Acronyms document contains definitions of acronyms that are not defined in this caveats document.
- Bug Navigator II—If you have an account on Cisco Connection Online (CCO), you can use Bug Navigator II to find caveats of any severity for any release. Access Bug Navigator II at http://www.cisco.com/support/bugtools, or from CCO by logging in and selecting **Service & Support**: **Technical Assistance Center**: **Software Bug Toolkit**: **Bug Navigator II**.
- *Release Notes for Cisco IOS Release 12.0*—These release notes describe new features and significant software components for Cisco IOS software Release 12.0. All features in Cisco IOS Release 12.0 are also in Cisco IOS Release 12.0 T.
- *What's Hot for Cisco IOS Software Release 12.0—What's Hot for Cisco IOS Software Release 12.0* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.0 and Release 12.0 T. If you have an account on Cisco Connection Online (CCO), you can access *What's Hot for Cisco IOS Software Release 12.0* from CCO by logging in and selecting **Service & Support**: **Software Center**: **Cisco IOS Software**: **Cisco IOS 12.0**: **What's Hot for Cisco IOS Software Release 12.0**.

Note Release notes are only modified on an as-needed basis. The maintenance release number and the revision date represent the last time the release notes were modified to include new or updated information. For example, release notes are modified whenever any of the following items change: software or hardware features, feature sets, memory requirements, software deferrals for the platform, microcode or modem code, or related documents.

The following table lists the most recent release notes when this caveats document was published:

Release Notes	Cisco IOS Release	Revision Date
Release Notes for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for Cisco 2600 Series for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for Cisco 3600 Series for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for the Cisco MC3810 for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for Cisco 4000 Series for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for Cisco AS5200 Universal Access Servers for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000

Release Notes	Cisco IOS Release	Revision Date
Release Notes for the Cisco AS5300 for Cisco IOS Release 12.0	Release 12.0(14)	November 6, 2000
Release Notes for the Cisco AS5800 for Cisco IOS Release 12.0	Release 12.0(1)	October 26, 1998
Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.0	Release 12.0(3)	February 8, 1999

Open Caveats—Cisco IOS Release 12.0(14)

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(14). All the caveats listed in this section are open in Cisco IOS Release 12.0(14). This section describes severity 1 and 2 caveats and select severity 3 caveats.

AppleTalk

- CSCds04435

  A Cisco 3640 router running Cisco IOS Release 12.0(12) reloads in atroute_GetValidEqualPath when enabling switched virtual circuits (SVCs). There is no workaround.

Basic System Services

- CSCdj14601

  When hardware compression is enabled, packets are normally fast-switched. If you disable fast switching and then enable fast switching again, fast switching remains disabled.

  Workaround: Reconfigure hardware compression by entering the **no compression** command followed by the **compression stac** command.

- CSCdm36098

  On a Versatile Interface Processor (VIP) with PA-4T+ port adapter and compression service adapter (CSA) that are configured with distributed weighted fair queueing (dWFQ), a severe performance degradation will occur that you can diagnose by the numerous packet drops. This situation occurs when the interface is under heavy traffic.

  Workaround: Always enable the CSA first, and then enable dWFQ.

- CSCdm69245

  A Cisco router may reload because of a timer corruption. There is no workaround.

- CSCdm71775

  If you issue the **write erase** command which erases the configuration in NVRAM, the boot variables are not changed.

  Workaround: Change the boot configuration and configuration register, and then save the configuration before erasing NVRAM.

- CSCdp32560

  A Cisco router that is running Cisco IOS Release 12.0(5.5) with a Route Switch Processor (RSP) may see “output stuck” messages followed by a “CBus complex restart” message that clears the problem. There is no workaround.

- CSCdp59691

  A Cisco AS5800 series universal access server, a Cisco 7200 series router, a Cisco uBR7200 universal broadband router, or a Cisco 6400 series router may experience a memory leak. If an IP packet needs fragmentation in the fast-switching path and the packet has additional bytes of data tagged on beyond the length indicated in the IP header, there might be a leak in the I/O memory of the system. The memory leak will depend on the size of the original unfragmented packet and on the size of the extraneous data.

  Workaround: Disable fragmentation in the fast-switching path by using the **service disable-ip-fast-frag** global configuration command.

- CSCdr17966

  When the **aaa new-model** global configuration command is not present in the startup configuration mode, command authorization fails because the authentication, authorization, and accounting (AAA) software cannot find a username.

  Workaround: Enter the **aaa new-model** global configuration command in the startup configuration.

- CSCdr22407

  Frame Relay (FRF.9) hardware compression does not keep input byte count for compressed data on both interface level and Frame Relay permanent virtual circuit (PVC) level. The display from these commands appears inconsistent with the output byte counts and with the FRF.9 software compression statistics displayed by the **show interface**, **show compress**, and **show frame-relay pvc** EXEC commands. Also, the corresponding MIB representation becomes inconsistent. There is no workaround.

- CSCdr28133

  After an upgrade from Cisco IOS Release12.01XA3 to Cisco IOS Release 12.0(7)T, a StrataCom backbone with UXM trunk cards needs two ATM cells instead of one for the fax frame size, thereby taking 25% more bandwidth. There is no workaround.

- CSCdr31580

  Memory leaks in a Cisco router that is running Cisco IOS Release 12.0(10)S and that is running a high number of ISDN data calls using Multilink PPP will eventually result in a system reload or degradation when memory is depleted.

  The processes in the **show process memory** EXEC command that continue to consume large amounts of memory are Multilink Event, PPP Manager, PPP Auth, and ISDN. There is no workaround.

- CSCdr47327

  When the compression service adapter (CSA) for a Cisco 7200 series router is configured with PPP encapsulation, it loses compression from the configuration upon router reload.

  Workaround: Reenable the **compress stac** interface configuration command after reload.

- CSCdr55787

  SA-ENCRYPT does not work if configured with fast switching or Cisco Express Forwarding (CEF) on a Cisco 7200 series router with hardware encryption (Cisco Encryption Technology).

  Workaround: Configure as process switching.

- CSCds13085

  A Cisco 7500 series router running Route Switch Processor (RSP1) and Cisco IOS Release 12.0(10) may experience the following reload and spurious alignments:

  ```
  System was restarted by bus error at PC 0x601B72E8, address 0x40000060 RSP Software
  (RSP-DSV-M), Version 12.0(10), RELEASE SOFTWARE (fc1) Image text-base: 0x60010930,
  data-base: 0x60D52000

  Stack trace from system failure: FP: 0x613576E0, RA: 0x601B72E8 FP: 0x61357850, RA:
  0x6029F13C FP: 0x613578D0, RA: 0x6026E790 FP: 0x61357A08, RA: 0x6029F13C

  RSP Software (RSP-DSV-M), Version 12.0(10), RELEASE SOFTWARE (fc1)

  Address Count Traceback 37C 1 0x605E95BC 0x60604B10 0x60604BF0 0x60605268 0x606053F4
  0x60250104 0x602500F0 14 1 0x601B72DC 0x6029F13C 0x6026E790
  ```

  There is no workaround.

- CSCds17029

  A Cisco 2509 router running Cisco IOS Release 12.0(12) that is configured as an access server may experience a buffer leak in big buffers:

  ```
  Big buffers, 1524 bytes (total 1030, permanent 50): 0 in free list (5 min, 150 max
  allowed) 1056 hits, 376 misses, 0 trims, 980 created 42 failures (0 no memory)
  ```

  The router runs short of I/O memory and has to be reloaded. There is no workaround.

- CSCds20054

  A Cisco 7200 series router running Cisco IOS Release 12.0(12) may experience a software-forced reload. There is no workaround.

- CSCds31059

  A Cisco 7500 series running Cisco IOS Release 12.0(11) images produces the following error message:

  ```
  RSP-2-QAERROR: reused or zero link errors.
  ```

  The problem occurs infrequently and is only related to using PA-2FEISL as two port FE adapter, which is not recommended.

  There is no workaround.

- CSCds45910

  A Route Switch Processor version 2 (RSP2) running Cisco IOS Release 12.0(9) may experience a buffer leak in the middle buffers. This buffer leak may cause the router to hang when the router runs out of memory. There is no workaround.

- CSCdr91706

  A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to "<code>http://router-hostname-or-IP-address/more-text?/ </code>" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

  This is not the same defect as CSCdr36952.

  The vulnerability, identified as Cisco Bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software Releases 12.0 through 12.1, inclusive. The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect.

  This vulnerability can be exploited only if the enable password is known or is not set.

The complete advisory is available at http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml.

- CSCds46280

  TFTP will not transfer a file greater then 16 MB to or from a Cisco router.

  Workaround: Use remote copy protocol (RCP) or File Transfer Protocol (FTP) to transfer the file.

- CSCds57060

  Tracebacks appear when fair queueing is configured on an ATM interface. There is no workaround.

EXEC and Configuration Parser

- CSCds11268

  Under certain circumstances, the CPU utilization for the process corresponding to the EXEC session on a Cisco AS5300 series universal access server increases to more than 90 percent if a dialup EXEC session pauses indefinitely. There is no workaround.

IBM Connectivity

- CSCdp19205

  If you connect a Route Switch Module (RSM) to a PIX Firewall in a multiring environment and configure the RSM using the **multiring trcrf-vlan** interface configuration command and the **multiring all** interface configuration command, the RSM might lose the connection to the PIX Firewall. In this situation, the RSM cannot ping the PIX Firewall. A sniffer trace reveals that the RSM is sending the Address Resolution Protocol (ARP) request as a single route explorer and that the PIX Firewall is answering with a directed frame. However, the control byte in the Routing Information Field (RIF) of this directed response is set to 46 instead of 06 (where 6 is the length of the RIF), and the RSM discards the packet.

  Workaround: Configure the RSM by entering the **multiring all all-routes** interface configuration command. This command will instruct the RSM to send the initial ARP request as an all-route explorer, and the PIX Firewall will respond with a directed frame that has the control byte in the RIF set to 06. The RSM will accept this frame.

- CSCdp20000

  A Cisco router that is running Cisco IOS Release 11.2(15a) or Cisco IOS Release 11.2(15a)P may reload with a bus error. There is no workaround.

- CSCdp94309

  A Cisco Route Switch Processor (RSP) that is running Cisco IOS Release 12.0(9) may reload with a bus error when you use the **debug fras state** EXEC command. A Cisco RSP may also reload if debug commands are not enabled. There is no workaround.

- CSCdr55235

  In some circumstances, Frame Relay access support (FRAS) fails to get connected. The output of the **show llc** command shows that the Logical Link Control (LLC) session remains in Asynchronous Disconnect Mode (ADM).

  Workaround: Remove the failing FRAS connection from the configuration and then add it back in to remove the LLC session.

- CSCdr87403

  When Advanced Peer-to-Peer Networking (APPN) virtual data-link control (VDLC) is configured between Cisco 3640 routers and AS/400s, there is a problem if all the network nodes (NN) are using High Performance Routing (HPR) and there is a data-link switching (DLSw) Lite circuit established between the Cisco 3640 data-link switching (DLSw) peers. The High-Performance Routing data-link switching (HPR/DLSw) circuit will time out according to the 10 minute timeout of Lite circuits (for example, when they perform an initial program load (IPL) on the AS/400s).

  Consequently, this link can never be brought back up again unless you stop/start the Advanced Peer-to-Peer Networking/Virtual Data-Link Control (APPN/VDLC) link or clear the DLSw circuit (the one for the CP-CP sessions using SAP.04.) so that no data traffic is possible between the AS/400s. There is no workaround.

- CSCds17085

  Under rare circumstances there may be an invalid Routing Information Field (RIF) when using Data-Link Switching/Routing Information Field (DLSw/RIF) pass-through is used. As a consequence the llc2 session between the Network Control Protocols or the virtual telecommunications access methods (VTAM) do not get established.

  Workaround: Use remote source-route bridging (RSRB) without local-ack.

- CSCds17994

  A Cisco 7200 series router displays duplicate ring violation messages when the **debug source event** command is enabled, even though there is no duplicate ring at all. There is no workaround.

- CSCds18933

  When mainframe is shut down and subchannels are still active, a network outage occurs in that a Multipath Channel transmission group (MPC TG) becomes inactive. During the reactivation of the transmission group (TG), the following error message is produced:

  ```
  %RSP-3-RESTART: interface Channel4/2, output stuck
  ```

  This error message could also be experienced during the configuration of a new Cisco MPC TG. There is no workaround.

- CSCds26826

  A Route Switch Processor version 4 (RSP4) running Qualified Logical Link Control may reload under heavy loads when an initial program load (IPL) is done on the HOST to which the IPL is initiated through QLLC or X.25. There is no workaround.

- CSCds26887

  An Advanced Peer-to-Peer Networking (APPN) router with the Fast Ethernet Inter-Switch Link (ISL) interface sometimes uses an incorrect virtual LAN number in the ISL header of the APPN packets. There is no workaround.

- CSCds47841

  A Cisco 2600 series router running Cisco IOS Release 12.0(13.3) may reload when running data-link switching (DLSw). This happens only in a DLSw border peer network with peers on demand that frequently get established and shut down. There is no workaround.

Interfaces and Bridging

- CSCdk48089

  Removing an ATM Deluxe card from a Cisco 7200 series router and inserting an ATM Lite card in the same slot may cause the router to fail. There is no workaround.

- CSCdr47324

  With fast switching (Optimum, Cisco Express Forwarding (CEF), or flow) enabled, a Cisco 7200 series router may fail to route packets larger than 1496 bytes from any Fast Ethernet (FE) interface and a Bridge Group Virtual Interface (BVI). It is also possible that the first packet may reach its destination (because it is process-switched), but all subsequent packets will fail.

  Workaround: Disable fast switching on the FE interface.

- CSCdr57358

  An Inter-Switch Link (ISL) trunk does not work between a Cisco Catalyst 5500 and a Cisco 7000 series router that is running Cisco IOS Release 12.0.7, 12.0.8, or 12.0.11 with a PA-FE-TX port adapter that performs ISL in software microcode. This port adapter appears in the output of the **show diag** privileged EXEC command as 100BASE-TX-nISL. The ISL trunk works on the PA-FE-TX port adapter that appears in the output of the **show diag** privileged EXEC command as 100BASE-TX-ISL and supports ISL in hardware.

  Workaround: Create an 802.1Q trunk.

- CSCds14572

  With an ATM Lite Port Adapter (PA), permanent virtual circuit (PVC) discovery fails to come up with the right PVC parameters for variable bit rate-non real-time (VBR-NRT) service category. This problem happens only for the ATM lite interface. There is no workaround.

- CSCds14583

  A six-port CX-Ethernet Interface Processor (EIP) reloads randomly. Ports are shut down and you must enter the **no shut** command to bring them back. The following traceback errors are generated in the log:

```
%SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current co nfiguration to
10.110.214.21
%STANDBY-6-STATECHANGE: Standby: 1: Ethernet3/0 state Standby - > Active
%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot 3, cmd code 32 -Traceback=
60289C38 6028A124 60282DB8 60283AC0 60283A98 6028DD20 603A9610 603A9 A00 603A9CBC
603AB3E8 60221844 60221830
%CBUS-4-RSETFAIL: Interface Ethernet3/0 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
%CBUS-4-RSETFAIL: Interface Ethernet3/0 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
%CBUS-3-ADDRFILTR: Interface Ethernet3/0, address filter select command failed, code
0x8010 -Traceback= 6028DC08 6028DD10 603A9630 603A9A00 603A9CBC 603AB3E8 60221844 60221
830
%CBUS-4-RSETFAIL: Interface Ethernet3/0 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
%STANDBY-6-STATECHANGE: Standby: 1: Ethernet3/3 state Standby - > Active
%CBUS-4-RSETFAIL: Interface Ethernet3/3 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010 %CBUS-4-RSETFAIL: Interface Ethernet3/3
failed to reset properl y in cbus_mci_record_ether_address(), code 0x8010
%CBUS-4-RSETFAIL: Interface Ethernet3/3 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
%CBUS-4-RSETFAIL: Interface Ethernet3/3 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
```

```
%STANDBY-6-STATECHANGE: Standby: 1: Ethernet3/5 state Standby - > Active
%CBUS-4-RSETFAIL: Interface Ethernet3/5 failed to reset properl y in
cbus_mci_record_ether_address(), code 0x8010
```

There is no workaround.

- CSCds37758

  On a Cisco router that is running Cisco IOS Release 12.1(4.2) or a later release, Intermediate System-to-Intermediate System (IS-IS) will fail to form an adjacency over a 16 MB Token Ring link.

  Workaround: Set the Connectionless Network Service (CLNS) maximum transmission unit (MTU) size to 4461 on the Token Ring interfaces by entering the **clns mtu 4461** interface configuration command.

- CSCds44777

  On a Cisco 7500 series router running Cisco IOS Release 12.0(7)T or 12.0(10) with Port Adapter 4T+ (PA-4T+), Fast Serial Interface Processor (FSIP), or Port Adapter 8T (PA-8T), Dedicated Token Ring (DTR) Port Adapter does not drop and continuously pulses according to the configured **pulse-time x** interface configuration command time intervals. Also, on FSIP and PA-4T+ the RSP-3-RESTART message appears right before a router has to be rebooted to recover a serial interface from a circuit outage that was configured for **pulse-time x** interface configuration command. There is no workaround.

- CSCds45168

  After a development engineer (DE) special is applied on Cisco IOS Release 12.0 (12) that integrated CSCds07197, problems occur with Tip/Ring (T/R) network applications. End-to-End Systems Network Architecture (SNA) applications fail with link failures. Sniffer traces show a frame larger than 4472. There is no workaround.

- CSCds51651

  A Cisco 7500 series router may fail due to a software-forced reload if both FRF.9 hardware compression and weighted fair queuing are configured on the same serial link. There is no workaround.

IP Routing Protocols

- CSCdp02880

  A Route Processor running Cisco IOS Release 12.0 prevents (S,G,RP) “prune” messages from keeping the (S,G) state alive. This situation occurs when edge routers are running Protocol Independent Multicast version 1 (PIMv1) and do not perform periodic data-header-registers to the Route Processor. Interoperability between PIMv2 and PIMv1 may be affected by this problem. There is no workaround.

- CSCdp05523

  If the address range defined in a Network Address Translation (NAT) pool is large, CPU utilization may rise to 100 percent. If a large number of translations are still in the NAT table showing large expiration timeout values, then the entries were not exited properly.

  Workaround: Specifically putting a reduced TCP translation timeout (20 to 30 minutes) has shown improvement. Apparently there are a lot of TCP translations that were not exited properly and the default timeout of 24 hours would leave these translations hanging. Reducing the translation timeout clears the entries earlier. Split the address range into smaller ranges, and define more NAT pools.

- CSCdp71893

  A (S,G) entry created by receipt of data on an interface will have a NULL outgoing interface list. Unless the X-flag is set for this entry, the entry expiration time will not be updated and X-flag will time out and then be recreated by the next data packet. This condition may increase the CPU usage on routers that see multicast packets for a large number of sources. There is no workaround.

- CSCdr02975

  The Cisco router has a CPU hog when there are a large number of link-state advertisement (LSA) deletions. Two autonomous systems (AS) were accidentally merged. When they were restored, the CPU hogged while removing 60,000 link-state advertisements (LSA). There is no workaround.

- CSCdr54230

  A Border Gateway Protocol (BGP) update contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

  The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the extended length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

  The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASes) in the segment. The path segment value contains the list of ASes (each AS is represented by two octets).

  The total length of the attribute depends on the number of path segments and the number of ASes in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASes (without having to use the extended length bit) is 126 [=(255-2)/2]. If the update is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

  The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its internal Border Gateway Protocol (BGP) peers would detect the mismatch and issue a notification message (update malformed) to reset their session.

  The average maximum AS_PATH length in the Internet is between 15 and 20 ASes, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

- CSCdr73140

  After Cisco IOS software bootup, Open Shortest Path First (OSPF) may create a link-state advertisement (LSA) for an interface that is in the “interface up, line protocol down” state. This problem does not occur if you administratively shut down the interface at boot time and then later bring it up.

  Workaround: Administratively shut down the interface, save using the **copy system:running-config nvram:startup-config** command, and reboot the router.

  Alternate workaround: Exclude the interface address from OSPF by removing the network statement or restricting your inverse mask.

- CSCdr79512

  A summary link-state advertisement (LSA) with an abnormally low metric is generated by an area border router (ABR). This situation may be spuriously generated. There is no workaround.

- CSCds38006

  Unicast traffic fails on a specified interface when the **ip mroute-cache** command in interface configuration mode is used.

  Example:

  ```
  interface FastEthernet3/0/0 ip address 4.4.4.4 255.255.255.0 ip pim sparse-dense-mode
  ip route-cache distributed ip mroute-cache distributed

  ping 4.4.4.5

  Type escape sequence to abort.

  Sending 5, 100-byte ICMP Echos to 4.4.4.5, timeout is 2 seconds: ..... Success rate is
  0 percent (0/5)
  ```

  Workaround: Disable multicast distributed switching at interface. Use multicast fast switching instead.

- CSCds38187

  A Cisco router may appear to fast-switch multicast traffic. When the router is configured for distributed switching, the following command output is produced:

  ```
  ! interface FastEthernet3/0/0 ip address 4.4.4.4 255.255.255.0 ip pim sparse-dense-mode
  no ip route-cache distributed ip mroute-cache distributed

  wac-7513#sh int fa3/0/0 stat FastEthernet3/0/0 Switching path Pkts In Chars In Pkts Out
  Chars Out Processor 3192 408632 13005 1188753 Route cache 0 0 32400 3693600 Distributed
  cache 0 0 0 0 Total 3192 408632 45405 4882353
  ```

  Continue to fast-switch until a Cisco IOS upgrade release is available.

  There is no workaround.

- CSCds39835

  After interface flap, the Open Shortest Path First (OSPF) state for the interface may remain down. This condition can be seen through the **show ip ospf** EXEC command.

  Workaround: Restart the OSPF process.

- CSCds41217

  On Cisco 7507 and 7206 routers running Cisco IOS Release 12.0.12, Open Shortest Path First (OSPF) shows the neighbor as full, but pinging the neighbor that shows up with “full” status under **show ip ospf neighbor** EXEC command, comes back with 20 to 50 percent packet loss. The neighbor is connected to the core router via an ATM link. The core router is the router that has the problem. Other neighbors on the router do not display the same symptom; only the two routers on the ATM0/0/0.1 & ATM0/0/0.2 of the cCore0.msp have this problem.

  There is no workaround.

Miscellaneous

- CSCdj88434

  A router may reload when bad packets, whose datagram size is smaller than the IP total length carried in the IP header, are received by the router and also classified for encryption. This situation affects Cisco Encryption Technology (CET) only; it does not affect IP Security (IPSec).

  Workaround: Upgrade to Cisco IOS Release 12.1(4).

- CSCdk18888

  A VIP Token Ring interface does not encrypt or decrypt IP packets containing a Routing Information Field (RIF), even though the initial encryption connection setup with the remote router is successful. Encryption and decryption for Token Ring IP packets without a RIF continue to function normally. There is no workaround.

- CSCdm01831

  A timing problem exists that is specific to the Route Switch Module (RSM). If an interface MAC address changes, the code may not perform all of the bring-up functions, such as enabling IPX routing on the interface. In this case, issuing the **show ipx route** user command in EXEC mode shows that the problem VLAN network is not in the routing table.

  Workaround: Go to the interface and deconfigure the IPX network, and then reconfigure the IPX network.

- CSCdm81058

  A Cisco 3640 router may reload with a bus error at PC 0x603DFF38, address 0xAC, and stack decode show the following:

  ```
  [fcp_transmit_on_mgmt_idbs [fcp_transmit_shm_msg [fcp_reenable_learning
  [fcp_process_sh_ack_msg [fcp_input [fcp_process [r4k_process_dispatch
  [r4k_process_dispatch
  ```

  There is no workaround.

- CSCdm87751

  If integrated routing and bridging (IRB) is being used between an Ethernet Interface and a Token Ring Interface, the Bridge Group Virtual Interface (BVI) may not respond to any IP frames originating on the Token Ring. This condition occurs if the BVI is sharing the MAC layer address of the Token Ring interface.

  Workaround: Change the MAC layer address of the BVI to a different LAN interface that is participating within the same bridge group. Enter the **mac-address** interface configuration command on the BVI interface, or reload the router, which will use the first active LAN interface within the bridge group.

- CSCdp03254

  Cisco routers running IP Security (IPSec) may reload if certificates are enrolled with a fully qualified domain name (FQDN) identity that has no IP address or router serial number. The FQDN of the router is changed, and certificates are reenrolled with the new FQDN identity (no IP address or router serial number).

  Workaround: Include the IP address and the router serial number in the second enrollment request.

- CSCdp05975

  On a Cisco LightStream 1010 that is running Cisco IOS Release 11.3 or Cisco IOS Release 12.0, virtual circuit (VC) merge does not work properly. Several cyclic redundancy check (CRC) errors appear when VC merge is active and traffic is present. There is no workaround.

- CSCdp55089

  Cisco 2600/3600 series routers may get a spurious access error while using the **no** form of the **smds dxi** interface configuration command. There is no workaround.

- CSCdp86385

  A Cisco RSP4 Route Switch Processor (RSP) that is running Cisco IOS Release 12.0(9) may reload when you reboot. There is no workaround.

- CSCdp92097

  Cisco Encryption Technology (CET) may not work when weighted fair queueing (WFQ) is configured on the interface of which crypto map is applied. There is no workaround.

- CSCdp95227

  If you make a call from a Cisco AS5300 series universal access server that is running Cisco IOS Release 12.0(7)T, you may not hear a ringback. The Cisco 3640 router that is running Cisco IOS Release 12.0(7)XK at the remote end rings, but there is no voice path. You see a disconnect code of "IE out of order" or "IE invalid length message" on the called end. The output of the **debug isdn q931** EXEC command shows "IE invalid" on the AS5300 universal access server. There is no workaround.

- CSCdr05668

  With some protocols, a packet may have its Time To Live (TTL) decremented an extra time. This situation occurs only in transport mode while broadcasting Open Shortest Path First (OSPF) HELLO packets.

  Workaround: Use tunnel mode or a different routing protocol.

- CSCdr42549

  With distributed Cisco Express Forwarding (deceive) enabled, the input counters on the **show interfaces** EXEC command may overcount packets on a Versatile Interface Processor (VIP) channelized serial interface and display the following results:

```
---------------------------------------- vip2c2#clear counters Clear "show
interface" counters on all interfaces [confirm] vip2c2#sh int ser4/0/0:0 stat
Serial4/0/0:0 Switching path Pkts In Chars In Pkts Out Chars Out Processor 0 0 0 0 Route
cache 0 0 0 0 Distributed cache 0 0 0 0 Total 0 0 0 0 vip2c2#sh int hssi12/0 stat Hssi12/0
Switching path Pkts In Chars In Pkts Out Chars Out Processor 3 411 2 368 Route cache 0
0 0 0 Distributed cache 0 0 0 0 Total 3 411 2 368 vip2c2#sho run int ser4/0/0:0 Building
configuration...

Current configuration: ! interface Serial4/0/0:0 ip address 22.0.0.2 255.0.0.0 no ip
directed-broadcast no ip route-cache distributed no keepalive no fair-queue end

vip2c2# ---------------------------------- vip2c1#ping Protocol [ip]: Target IP
address: 192.192.192.1 Repeat count [5]: 500 Datagram size [100]: 1015 Timeout in
seconds [2]: Extended commands [n]: Sweep range of sizes [n]: Type escape sequence to
abort. Sending 500, 1015-byte ICMP Echos to 192.192.192.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 292/304/1580 ms vip2c1#
------------------------------------ vip2c2#sh int hssi12/0 stat Hssi12/0 Switching
path Pkts In Chars In Pkts Out Chars Out Processor 27 3978 23 3812 Route cache 500 509500
500 507500 Distributed cache 0 0 0 0 Total 527 513478 523 511312 vip2c2#sh int ser4/0/0:0
stat Serial4/0/0:0 Switching path Pkts In Chars In Pkts Out Chars Out Processor 10 3190
10 3100 Route cache 500 509500 500 507500 Distributed cache 0 0 0 2000 Total 510 512690
510 512600 vip2c2#
```

  There is no workaround.

- CSCdr49748

  A Cisco 2600 series router may lose the startup configuration because of NVRAM corruption and report the following error at the **show startup-config** command:

```
%% Non-volatile configuration memory has not been set up or has bad checksum
```

Workaround: Execute a **write memory** EXEC command or a **copy running start** command if you see this kind of error message.

- CSCdr79628

  When IP Security (IPSec) is being enabled on a Cisco 7507 router running Cisco IOS Release 12.0.11 code, the following messages appear on the console:

  ```
  Jul 8 11:20:03: %SYS-3-NULLIDB: Null IDB in ipsendnet -Process= "Encrypt Proc", ipl= 0, pid= 62 -Traceback= 6034DD1C 60C1CC80 60C08CB0 60C0818C 60221844 60221830 Jul 8 11:32:38: %SYS-3-NULLIDB: Null IDB in ipsendnet -Process= "Encrypt Proc", ipl= 0, pid= 62
  ```

  A traceback is seen, but the functionality does not seem to be affected.

  There is no workaround.

- CSCdr79785

  A loss of connectivity occurs on a Cisco 7500 series router running Cisco IOS Release 12.0 S when the **tag-switching ip** command is enabled on a router or when tag packets are being switched by the Interface Processor even when they are expected to be switched by the Route Processor. This situation occurs only when distributed switching is turned off (the no **ip cef distributed** global configuration command or the **no ip route-cache distributed** interface configuration command is enabled).

  Workaround: Enable distributed switching with the **ip cef distributed** command if tag switching is enabled (**tag-switching ip**) on the router.

- CSCdr81283

  Context-based Access Control (CBAC) may cause Hypertext Transfer Protocol (HTTP) sessions to fail in some cases. There is no workaround.

- CSCdr84440

  A Cisco router reloads with a bus error at PC 0x60352FFC(pot1e1_safe_start), address 0x0. There is no workaround.

- CSCdr87348

  A Cisco router running Cisco IOS Release 12.0(10) may experience a software-forced reload without any configuration changes. There is no workaround.

- CSCdr89618

  A Cisco Route Switch Processor (RSP2) running RSP Software (RSP-DSV-M), under Cisco IOS Release 12.0(9) may experience a memory leak in the dead process. This process may hold up to 35M. You can verify this situation by using the **show memory dead** command. There is no workaround.

- CSCdr93496

  A router using Connectionless Network Service (CLNS) routing on a Bridge Group Virtual Interface (BVI) may reload after you use the **no shutdown** interface configuration command on the BVI. There is no workaround.

- CSCdr93896

  A Cisco 12000 series router running Cisco IOS Release 12.0(11)S3 reloads 2 to 3 times per week with memory corruption. There is no workaround.

- CSCds01012

  When sending IPSec traffic across a second channel while the first channel is still up and passing IPSec traffic, a Cisco router may stop passing traffic altogether. This condition has been observed in the following situation:

  – There are two central sites (A and B in this example) with Cisco 3640 routers that are running Cisco IOS Release 12.0(7)XK1.

  – There is a remote site with a Cisco 2621 router that is running Cisco IOS Release 12.0(7)XK1.

  – NAT and ML-PPP are not enabled.

  – Fast switching is disabled on all interfaces.

  – Crypto maps are applies to physical and virtual interfaces.

  – The two central sites are connected to the same OSPF area (backbone).

  – Each central site router has a PRI that the remote sites terminate on.

  – One remote site has a single BRI with two channels.

  – One channel is used to connect to the site A central router, and the other channel is used to connect the site B central router.

  – Certain traffic goes through site A, and other traffic goes through site B.

  The two links function properly when IPSec is not enabled on either link, or if IPSec is only enabled on one link. The traffic is still passed properly if IPSec is enabled on both links if all traffic is being routed through the main link. If the main link (the first BRI channel) goes down, it fails over to the backup link, and the traffic is IPSec encrypted. There is no workaround.

- CSCds03292

  When the committed access rate (CAR) is configured at the input of an interface using Frame Relay or High-Level Data Link Control (HDLC) encapsulation on Engine 0 POS LC, the throughput of the interface is 370 Mb/sec for a 256 byte packet. There is no workaround.

- CSCds04232

  A PA-A3-OC3MM= port adapter (PA) may not be recognized by a Cisco Catalyst 5500 series switch. The Versatile Interface Processor (VIP) reloads with a bus error when the PA is inserted. There is no workaround.

- CSCds09499

  Cisco IOS Software allocates calls to modems in the disconnecting state when it fails to find a free modem. Cisco IOS Software sends a terminate signal to a modem and after two seconds assumes that the modem is back to idle even if it does not receive an idle signal from the modem. This assumption is incorrect for modems taking longer to terminate and for modems that have failed. This situation results in RingNoAnswer (RNA) and a lower call success rate (CSR). There is no workaround.

- CSCds11055

  When Web Cache Communication Protocol (WCCP) is enabled on a Cisco 7500 series router running Cisco IOS Release12.0(11)S, that the router performance may be degraded, packets were lost on serial links, and internet connectivity may be lost. This situation may be related to the use of an Inter-Switch Link (ISL) interface. There is no workaround.

- CSCds16618

  Versatile interface processor (VIP) interfaces for Frame Relay subinterfaces and PPP interfaces are initialized much later than route processor (RP) interfaces after a router reloads.

None of the point-to-point adjacencies show up in the VIP for the serial port when the **show adjacency detail** EXEC command is used in the VIP slot console. Valid adjacencies are present in the RP and are displayed when the **show adjacency detail** command is issued on the main console.

Workaround: Enable only the **ip cef** global configuration command when you bring up the router. Then turn on the **ip cef distributed** command if needed. Pings are functional when just the **ip cef** command is configured.

Alternate workaround: After the router reloads, toggle the **ip cef distributed** configuration by entering the **no ip cef distributed** command, followed by the **ip cef distributed** command.

- CSCds16987

  Removing and then adding a channel group from the configuration of a PA-2CE1 port adapter may cause the output to stick followed by a cbus complex; thereby producing the following error message:

  ```
  %RSP-3-RESTART: interface Serial4/0/1:11, output frozen
  %RSP-3-RESTART: interface Serial4/0/1:12, output stuck
  %RSP-3-RESTART: cbus complex
  ```

  There is no workaround.

- CSCds23223

  A configuration involving an ingress professional services automation (PSA) access list(ACL) on one line card, combined with an output ACL and output committed access rate (CAR) on another line card, could result in a line card reload when traffic is passed through this path. There is no workaround.

- CSCds25711

  A Cisco 3640 router with 1- or 2-port network module NM-1E2W= may experience output queue wedged under load. There is no workaround.

- CSCds25745

  A Cisco 4700 series router with ATM and Ethernet interfaces reloads periodically while running Cisco IOS Release 12.0(12). There is no workaround.

- CSCds33876

  When using IP Security (IPSec), a Cisco 2514 router running Cisco IOS Release12.0(12) may reload unexpectedly with a software forced reload. Decoded tracebacks are consistent with memory corruption. There is no work around.

- CSCds34988

  It is possible on a Cisco gigabit switch router (GSR), that the 6 Port CT3 card experiences problems with the fabric weighted random early detection/Modified deficit round robin (WRED/MDRR) when there is congestion at the Egress of this Line Card. This is seen by applying WRED/MDRR on the fabric direction, however there will be no noticeable impact. This was experienced when running special image: gsr-p-mz.120-12.6.S2. There is no workaround.

- CSCds38804

  Some Sandisk 48 MB flash cards do not boot. There is no workaround.

- CSCds40078

  When Routing Information Protocol (RIP) is running on an interface, and the IP address is deconfigured, RIP stops running on the correct interface. After this situation occurs, if a new IP address is configured that falls under the RIP network statements, RIP will not start running on the interface again.

  Workaround: Deconfigure RIP, and reconfigure it again.

- CSCds41097

  On a Cisco router, the Token Ring interface gets wedged after upgrading from Cisco IOS Release 11.2 code.

  Workaround: Reload the router each time the problem occurs.

- CSCds41672

  Upon reloading a Cisco router that is using multiple tunnel interfaces and Cisco Encryption Technology (CET) over Frame Relay it is possible that the router may experience only part of the CET tunnels responding.

  Workaround: Using the **clear crypto connection** command in global configuration will allow the rest of the tunnels to respond.

- CSCds43080

  When NMHDV+WIC-2MFT-T1 is configured to support 48 calls using a connection trunk, and the voice activity detection (VAD) device is disabled, the trunked calls will begin to flap. There is no workaround.

- CSCds45328

  A small amount of memory will be allocated and not freed when the configuration is written to nonvolatile memory. There is no workaround.

- CSCds49667

  With distributed Cisco Express Forwarding (dCEF) enabled on an ATM subinterface, IfInOctets will appear to be decreasing whereas **show interfaces** privileged EXEC command as well as IfInPackets show increases. There is no workaround.

- CSCds51143

  An E1 Continuity Test (COT) in loopback mode fails. There is no workaround.

- CSCds52655

  On a Cisco 3620 router running Cisco IOS Release 12.0(6), the **no ip directed-broadcast** interface configuration command is configured on all interfaces, but the router still passes the **ip directed-broadcast traffic** command, and the following messages are produced:

  ```
  ! ! Last configuration change at 23:48:03 EDT Wed Oct 18 2000 ! NVRAM config last updated
  at 15:01:01 EDT Mon Oct 16 2000 ! version 12.0 service timestamps debug datetime
  localtime show-timezone service timestamps log datetime localtime show-timezone service
  password-encryption ! hostname NJEX3620R1 ! logging buffered 100000 debugging enable
  secret 5 $1$R9bN$15LGNLAwTxhWYFiFE2bHx/ ! ip subnet-zero no ip finger no ip
  domain-lookup ip host iops 208.222.92.52 ! ! ! clock timezone EST -5 clock summer-time
  EDT recurring ! ! ! ! interface Ethernet0/0 description Exodus_Network Infrastructure
  ip address 172.16.153.210 255.255.255.0 no ip directed-broadcast ! interface Serial0/0
  description T1 to Kaplan Corp. ip address 192.168.158.13 255.255.255.252 ip access-group
  101 in no ip directed-broadcast ! router eigrp 10 redistribute static network 172.16.0.0
  no auto-summary ! ip classless
  ```

  ```
  ip route 0.0.0.0 0.0.0.0 172.16.153.254 ip route 10.30.0.0 255.255.0.0 Serial0/0 ip
  route 172.16.150.0 255.255.255.0 Serial0/0 ip route 192.168.158.4 255.255.255.252
  Serial0/0 ip route 204.177.145.0 255.255.255.0 Serial0/0 ip route 208.222.92.0
  255.255.252.0 Serial0/0 ! logging 172.16.153.143 logging 208.222.93.179 access-list 1
  permit 208.222.92.86 access-list 1 permit 208.222.92.90 access-list 1 permit
  208.222.93.244 access-list 1 permit 208.222.94.237 access-list 1 permit 172.16.153.0
  0.0.0.255 access-list 101 permit ip 208.222.92.0 0.0.3.255 172.16.153.0 0.0.0.255 log
  access-list 101 permit ip 208.222.92.0 0.0.3.255 host 192.168.158.13 log access-list
  101 permit ip 204.177.145.0 0.0.0.255 172.16.153.0 0.0.0.255 log access-list 101 permit
  ip 204.177.145.0 0.0.0.255 host 192.168.158.13 log access-list 101 permit ip
  172.16.150.0 0.0.0.255 host 192.168.158.13 log access-list 101 permit ip 172.16.150.0
  0.0.0.255 172.16.153.0 0.0.0.255 log access-list 101 permit ip 192.168.158.4 0.0.0.3
  ```

```
172.16.153.0 0.0.0.255 log access-list 101 permit ip 192.168.158.4 0.0.0.3 host
192.168.158.13 log access-list 101 permit ip 10.30.0.0 0.0.255.255 172.16.153.0
0.0.0.255 log access-list 101 permit ip 10.30.0.0 0.0.255.255 host 192.168.158.13 log
! line con 0 password 7 060A5C354541195D0C1953 login transport input none line aux 0
password 7 0308081F0F003108470758 login line vty 0 4 access-class 1 in password 7
011F55105204164B28420F login ! ntp clock-period 17179758
```

```
login line vty 0 4 access-class 1 in password 7 011F55105204164B28420F login ! ntp
clock-period 17179758 ntp source Ethernet0/0 ntp master 6 ntp server 132.236.56.250
prefer ntp server 158.121.104.4 end
```

There is no workaround.

- CSCds54938

  A Cisco router connected to a server running CiscoSecure 2.431 reloads on a regular 24-to 48-hour basis because of a bus error at a low address. There is no workaround.

- CSCds59277

  The Configuration Extraction Tool (CET) between two Cisco 7206 routers running Cisco IOS Releases 11.2(19) and 12.0(11) may fail after a few minutes. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdk75507

  Some packets may not arrive at a destination when using Xerox Network Systems (XNS) fast switching over multiple equal-cost ATM paths. This situation can result in retransmission and connection timeouts.

  Workaround: Decrease the **xns maximum-paths** command in global configuration mode number to 1, or disable the **xns route-cache** command in global configuration mode on all interfaces in all of the paths.

- CSCdp28700

  If you change IPX encapsulation from Service Advertising Protocol (SAP) to Subnetwork Access Protocol (SNAP) on a dot1q subinterface over Fast Ethernet, you might receive “alignment correction” messages. There is no workaround.

- CSCdr00809

  A Cisco router may reload sporadically when it forwards a Type20 NetBIOS broadcast packet. There is no workaround.

- CSCdr89399

  After upgrading from Cisco IOS Release 11.2(16)P to Cisco IOS Release 12.0(10) Internetwork Packet Exchange (IPX) routing is unstable and causes connectivity problems and the following errors may occur:

  ```
  %DUAL-3-INTERNAL: IPX-EIGRP 1: Internal Error and %SYS-2-MALLOCFAIL: Memory allocation
  errors occuring.
  ```

  There is no workaround.

- CSCds51821

  When a Cisco 2500 series router is connected to basic-ni (isdn switch-type basic-ni) in Cisco IOS Release 12.0 (10) layer 2 flapping occurs. There is no workaround.

- CSCds54821

  A Cisco 4500 series router may have its memory fragmented because of Internetwork Packet Exchange (IPX). There is no workaround.

- CSCds56020

  A Windows PC with ISDN data Terminal Equipment Available (TA) dials into a Cisco AS5300 series universal access server for the purpose of receiving two ISDN calls for a PPP Multilink connection. The Cisco AS5300 series universal access server disconnects the first incoming ISDN call and initiates an outgoing ISDN call as Multi Service (MS) Callback is negotiated. Even as **dialer load-threshold 1 either** interface command is configured and the outgoing ISDN call is overloaded, the Cisco AS5300 series universal access server never initiates a second outgoing ISDN call. There is no workaround.

- CSCds56024

  A Windows PC with ISDN TA dials into an AS5300 with the purpose of receiving two ISDN calls for a PPP Multilink connection.

  The Cisco AS5300 series universal access server disconnects the first incoming ISDN call and initiates an outgoing ISDN call as MS Callback is negotiated. The Cisco AS5300 series universal access server also disconnects the second incoming ISDN call, but never initiates a second outgoing ISDN call even as MS Callback is again negotiated.

  There is no known workaround.

- CSCds57363

  Customer Queueing is configured on a Cisco router along with Frame Relay traffic shaping. When HTTP traffic is defined in the queues with custom queueing, the result is the slowing of other traffic. There is no workaround.

- CSCds59456

  Use of the **no ipx sap-uses-routing-info** command causes a loss of all Service Advertising Protocol (SAP) information inside a SAP table. A message seen when SAP debugging is enabled will show that SAP information is “rejected, route xxxx is not in table”.

  When the use of route information with service information is disabled, the SAP table will be ordered only by service hops information in the SAP packet and not by ticks or hops route metric.

  Do not disable the use of route information with service information until this is fixed. There is no workaround.

Protocol Translation

- CSCdk83758

  If you have protocol translation on vty and Dynamic Host Configuration Protocol (DHCP) proxy, and you configure IP unnumbered on the virtual template, DHCP fails. If you configure an IP address on the virtual template, DHCP succeeds. There is no workaround.

TCP/IP Host-Mode Services

- CSCds29458

  A Cisco 7500 series router with three Channel Interface Processor v2 (CIPv2) experiences a software-forced reload and the following error messages are produced:

  ```
  System was restarted by error - a software forced reload, PC 0x6023C070

  Route/Switch Processor (RSP) Software (RSP-JSV-M), Cisco IOS Release12.0(10), RELEASE
  SOFTWARE (fc1) Compiled Tue 21-Mar-00 00:34 by phanguye Image text-base: 0x60010930,
  data-base: 0x60EF6000

  Stack trace from system failure: FP: 0x61C9C270, RA: 0x6023C070 FP: 0x61C9C270, RA:
  0x6023A89C FP: 0x61C9C288, RA: 0x60243A00 FP: 0x61C9C2A0, RA: 0x60243D48 FP: 0x61C9C2D0,
  RA: 0x60238C68 FP: 0x61C9C2F8, RA: 0x603344C0 FP: 0x61C9C340, RA: 0x603350F8 FP:
  0x61C9C378, RA: 0x60331544

  The log in the reload information file displays the following error messages:

  Aug 24 09:05:58.642 UTC-08d: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x61C176BC
  -Process= "Exec", ipl= 0, pid= 27 -Traceback= 6032FC8C 6032C5F8 60334080 601B0B3C
  6033900C 603344D8 603350F8 60331544 60863C88 60870B90 6086427C 6033409C 601B0B3C
  6033900C 603344D8 603350F8 Aug 24 09:05:58.642 UTC-08d: %SYS-6-STACKLOW: Stack for
  process Exec running low, 0/12000 Aug 24 09:05:58.642 UTC-08d: %SYS-3-LOGGER_FLUSHED:
  System was paused for 00:00:00 to ensure console debugging output.
  ```

  The stack trace decodes as follows:

  ```
  0x6023C070:abort(0x6023c068)+0x8 Enter hex value: 0xRA::__start(0x60010000)+0x9fff0000
  0x6023A89C:crashdump(0x6023a88c)+0x10 Enter hex value:
  0xRA::__start(0x60010000)+0x9fff0000
  0x60243A00:process_run_degraded_or_crash(0x602439ac)+0x54 Enter hex value:
  0xRA::__start(0x60010000)+0x9fff0000
  0x60243D48:process_ok_to_reschedule(0x60243a30)+0x318 Enter hex value:
  0xRA::__start(0x60010000)+0x9fff0000 0x60238C68:edisms(0x60238c20)+0x48 Enter hex
  value: 0xRA::__start(0x60010000)+0x9fff0000
  0x603344C0:send_byte_block(0x60334448)+0x78 Enter hex value:
  0xRA::__start(0x60010000)+0x9fff0000 0x603350F8:tnof(0x60334c04)+0x4f4

  The tracebacks after the TCP-2-INVALIDTCB messages decode as follows:

  0x6032C5F8:tcp_close(0x6032c5e4)+0x14 0x60334080:close_connection(0x60333fb4)+0xcc
  0x601B0B3C:conn_session(0x601b0a3c)+0x100 0x6033900C:tty_status_ok(0x60338fb0)+0x5c
  0x603344D8:send_byte_block(0x60334448)+0x90 0x603350F8:tnof(0x60334c04)+0x4f4
  0x60331544:tcp_putc(0x60331410)+0x134 0x60863C88:_putchar(0x60863c20)+0x68
  0x60870B90:Ctputs(0x60870ac8)+0xc8 0x6086427C:tn3270_conn_terminate(0x6086421c)+0x60
  0x6033409C:close_connection(0x60333fb4)+0xe8
  0x601B0B3C:conn_session(0x601b0a3c)+0x100
  ```

  There is no workaround.

Wide-Area Networking

- CSCdk22864

  The **show cmns** EXEC command is no longer available in Cisco IOS Release 11.3. There is no workaround.

- CSCdk53369

  Under certain circumstances, a Cisco router will issue the following error message:

  ```
  "invalid P timer event".
  ```

  This can happen under certain versions of the code when X.25 switched virtual circuits (SVC) and a call are switched but not accepted. A call is received and forwarded, the reply is a clear packet that is returned to the originator. The originator typically sends a “clear confirm” then the message is not forwarded, leaving the other channel in the “clear-received state” (DCE/P6 or DTE/P7). The message is emitted some time after this exchange (based on the “call confirm” timeout DCE/T11 or DTE/T21). There is no workaround.

- CSCdk88854

  On a Cisco 7200 and 3600 series router, bridging over Frame Relay on a Basic Rate Interface (BRI) will fail when static mapping is configured for the permanent virtual circuit (PVC).

  Workaround: Use routing instead of bridging, or use a point-to-point subinterface.

- CSCdp31542

  On the ISDN PRI Switchtype for a 4ESS, primary-4ESS may not be fully compliant with certain vendor products. There is no workaround.

- CSCdp59816

  The X.25 over TCP (XOT) M-bit is ignored or dropped, so that all packets are corrupted. There is no workaround.

- CSCdp65474

  A Route Switch Processor 4 (RSP4) may reload with a bus error and a stack trace because of the X.25 protocol stack. This situation occurs only if X.25 Over TCP (XOT) is enabled, configured, and in use. This situation may occur on other platforms. There is no workaround.

- CSCdp68193

  When entering the **show tcp** EXEC command, a Cisco router that has a high X.25 protocol translation load may reload. There is no workaround.

- CSCdp97152

  When running Cisco IOS Release 12.0 with User-Network Interface (UNI) 3.0, a Cisco LightStream 1010 and a Cisco Catalyst 8540 MSR may fail to send poll protocol data units (PDUs) periodically. This situation may result in a

  ```
  no_response_timer expiry
  ```

  message and flapping of the Service-Specific Connection-Oriented Protocol (SSCOP) link.

  Workaround: Configure UNI 3.1 on the link.

- CSCdr15509

  A Cisco 3640 router may run out of small buffers in seven days with packets similar to the following packet:

  ```
  Buffer information for Small buffer at 0x60CAEF24 data_area 0x19D0C04, refcount 1, next
  0x0, flags 0x400200 linktype 55 (SRB), enctype 20 (FRAME-RELAY), encsize 34, rxtype 0
  if_input 0x60C0DD9C (Serial1/0), if_output 0x0 (None) inputtime 0x131FA530, outputtime
  0x0, oqnumber 65535 datagramstart 0x19D0C40, datagramsize 54, maximum size 260 mac_start
  0x19D0C40, addr_start 0x19D0C42, info_start 0x19D0C58 network_start 0x19D0C58,
  transport_start 0x19CA266 =20 =20 019D0C00: AFACEFAD 00000000 00010001 00000000
  /,o-............ 019D0C10: 00000000 60B6225C 00000000 00000000 .....6".........
  019D0C20: 00000000 00000000 00000000 00000000 ................ 019D0C30: 01000C00
  10000411 03008000 80C20009 .............B.. 019D0C40: 00400040 5DC028E9 AA000400
  C918AAAA .@.@]@(i*...I.** 019D0C50: 03000000 08060006 08000604 0001AA00
  ```

```
..............*. 019D0C60: 0400C918 011E1001 00000000 0000011E ..I.............
019D0C70: 10054378 0000AA00 0400C918 011E1001 ..Cx..*...I..... 019D0C80: 00000000
0000011E 10054378 0000300E ..........Cx..0. 019D0C90: 300C0608 2B060102 01010200
05000500 0...+.......... 019D0CA0: 636B0101 CD417A20 00000000 00000000 ck..MAz
........ 019D0CB0: 00000005 04B90000 00000000 00000000 .....9.......... 019D0CC0:
00000000 00000000 00000000 00000000 ................ 019D0CD0: 00000000 00000000
00000000 00000000 ................ 019D0CE0: 00000000 00000000 00000000 00000000
................ 019D0CF0: 00000000 00000000 00000000 00000000 ................
019D0D00: 00000000 00
```

There is no workaround.

- CSCdr36073

  A Cisco 7500 series router running Cisco IOS Release 12.0(9) may fail with a bus error if Multilink PPP (MLP) and IP Cisco Express Forwarding (CEF) are simultaneously enabled, and IP Security (IPSec) is used to provide IP layer encryption over the multilink interfaces. There is no workaround.

- CSCdr46335

  A Cisco 2500 series router that is running Cisco IOS Release 12.0(7) encounters negative input queue values under the interface. The router displays the following messages:

  ```
  Serial0 is up, line protocol is up Output queue 0/300, 0 drops; input queue -298/300,
  0 drops
  ```

  There is no workaround.

- CSCdr52732

  A Cisco router reloads when tearing down Link Access Procedure, Balanced (LAPB) from an X.25 reader/receiver. There is no workaround.

- CSCdr52853

  A Cisco router may reload with a SegV exception if an X.25 interface is misconfigured. There is no workaround.

- CSCdr71038

  A Cisco 2522 router that is running Cisco IOS Release 12.0(9) may experience a buffer leak in the big buffers.

  The datagram size is always 45 and the destination port 1723.

  ```
  pptp 1723/tcp pptp pptp 1723/udp pptp
  ```

  The following example illustrates this situation:

  ```
  Buffer information for Big buffer at 0x234ECC data_area 0x69A43C, refcount 1, next 0x0,
  flags 0x88 linktype 7 (IP), enctype 16 (PPP), encsize 1, rxtype 1 if_input 0x1FA7B8
  (Serial0.1), if_output 0x1CBEEC (Serial7) inputtime 0x0, outputtime 0x0, oqnumber 70
  datagramstart 0x69A48F, datagramsize 45, maximum size 1680 mac_start 0x69A48F,
  addr_start 0x0, info_start 0x0 network_start 0x69A490, transport_start 0x0

  source: 195.182.70.65, destination: 193.219.12.132, id: 0x45F7, ttl: 123, TOS: 0 prot:
  6, source port 1358, destination port 1723
  ```

  There is no workaround.

- CSCdr71279

  Pings fail across a back-to-back serial link unless the router is rebooted on a Cisco 7200 series router that is running Cisco IOS Release 12.0(5). There is no workaround.

- CSCdr72065

  A Cisco 7200 series Network Process Engine (NPE)-200 that is running Cisco IOS Release 12.0(9) reloads with a bus error and experiences several spurious access errors. There is no workaround.

- CSCds10234

  If you enter the **shutdown** interface configuration command on the E1 interface, it may cause a router to experience a software-forced reload. There is no workaround.

- CSCds22874

  When the LAN emulation layer on a Cisco 7200 series router receives wrongly formatted LAN emulation control frames, the following message is generated:

  ```
  %LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
  ```

  When the message is generated, LAN emulation clients may be shut down. There is no workaround.

- CSCds30874

  A Cisco 2610 router running Cisco IOS Release 12.1(5)T may reload with memory corruption when PPP multilink connections are tunneled via L2F across ISDN lines that are also running PPP multilink. There is no workaround.

- CSCds37204

  Under heavy traffic conditions, the WS-X6101 may not respond to the Marconi switch poll in a timely manner, and the Integrated Local Management Interface (ILMI) signaling will be restarted. This will also cause the Service-Specific Connection-Oriented Protocol (SSCOP) signaling to restart, and all virtual circuits (VC) will be torn down. There is no workaround.

- CSCds45511

  A Cisco 2610 router running Cisco IOS Release 12.0(12) reloads with a SegV exception at PC 0x80360428 when configuring ISDN dial backup.

  There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(14)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(14). This section describes severity 1 and 2 caveats and select severity 3 caveats.

IBM Connectivity

- CSCdr78455

  A Cisco router running data-link switching (DLSw) may reload with a SegV exception. This problem is specific to a DLSw border peer network. It does not happen with configured or promiscuous DLSw peers. The root cause is a memory leak when a peer on demand gets established and this peer establishing fails. If this happens repeatedly the router will finally run out of memory will be forced to reload.

  Workaround: Change the DLSw peer on demand inactivity timer

  dlsw peer-on-demand-defaults inactivity

  The maximum timeout configurable is 1440 minutes, which equals to 24 hours. This timeout controls how long the peer stays established after the last DLSw circuit goes away.

- CSCds27627

  NetBIOS frames with a payload of 47 to 59 bytes may be truncated when put onto Ethernet segments after being transported with DLSw Fast Sequenced Transport (FST) encapsulation. This occurs only on particle-based platforms (Cisco 3600 and 7200 series routers).

Workaround: Use DLSw with TCP encapsulation instead of FST encapsulation, or use a different router platform.

Interfaces and Bridging

- CSCdm45164

  Enabling Weighted Fair Queuing (WFQ) on an interface that belongs to a transparent bridging bridge group may cause packets that are egressing that interface to be sent out of order. This situation causes failure in terminated and bridged Logical Link Control 2 (LLC2) sessions.

  Workaround: Disable WFQ with the **no fair-queue** interface configuration command.

- CSCds07197

  On Cisco 2600, 3600, and 7200 series routers running Cisco IOS Release 12.1 and Release 12.1 T the maximum configurable transmission unit size under the Token Ring interface is 4464 bytes. There is no workaround.

- CSCds21753

  A Cisco router with a FDDI may corrupt some packets that are switched out of the FDDI. This problem has been confirmed only for the FDDI<->FDDI case with Multiprotocol Label Switching (MPLS) enabled. This problem may also affect FDDI<->ATM with MPLS, but is not confirmed for that case or any case other than FDDI<->FDDI with MPLS.

  Workaround: Keep a continuous stream of pings running from the router that is reporting the cyclic redundancy check (CRC) errors introducing the corruption targeted at the loopback address.

IP Routing Protocols

- CSCdr70471

  Open Shortest Path First (OSPF) allocates and deallocates memory for a variety of needs. If the problem persists, the system may end up with badly fragmented memory. The only solution at that time would be to reboot the router.

  Workaround: Reduce the number of link-state advertisements (LSA) in the OSPF database.

  Alternate workaround: Design a stable network, minimizing LSA withdrawals and reissue (that is, summarize routes into the core).

- CSCds23901

  For a multicast source directly connected to a router, the “R” flag is set when a (S,G,R) prune message is received if the (S,G) O-list is NULL 2. The prune message was received on the non-incoming interface (NON-IIF). This situation causes the incoming interface (IIF) to change to the Rendezvous Point (RP) and disconnects the IIF from the source. The “F” flag is reset. As a result the RP loses the S and G states and new receivers can not join the multicast source.

  Workaround: Configure the **ip pim rp-proxy-join** on the RP. This allows the RP’s S and G states to join the first-hop router and have the O-list populated. Multicast traffic will continue to flow to the RP but if the RP’s (S,G) O-list is NULL, it will fast-drop this traffic.

Miscellaneous

- CSCdk58757

  A Cisco router running Cisco IOS Release 12.0 and its branches reloads when a permanent virtual circuit (PVC) has more than one IP address associated with it. If one of the IP addresses is removed, an **inarp** command process is started. But if the PVC itself is removed the router will reload. There is no workaround.

- CSCdk68700

  Encryption over dialer profiles may cause a Cisco router to reload when fast switching is enabled. This situation results in a “get alignment fatal” error.

  Workaround: Disable fast switching on the dialer profile interfaces.

- CSCdr67651

  When removing a Hot Standby Router Protocol (HSRP) secondary address from an HSRP group, the primary HSRP address of that group will be removed from the Address Resolution Protocol (ARP) table, and the router will not respond to ARP requests for the HSRP primary address. This situation will lead to loss of connectivity for hosts that have not yet cached the HSRP MAC address.

  Workaround: Issue the **clear arp-cache** EXEC command on the interface after the HSRP address has been removed.

- CSCdr67801

  A Cisco 7200 series router or a Cisco 7500/RSP series router with a PA-A3 ATM port adapter may reload because of a bus error that points to an 0x50000000 address or an 0x08000000 address. These reloads occur after the PA-A3 driver has received a packet and attempts to process it.

  Workaround: Disable Cisco Express Forwarding (CEF) by entering the **no ip cef global** configuration command on the Cisco 7200 series router or by entering the **no ip cef** global configuration command on the Cisco 7500/RSP series router.

Protocol Translation

- CSCdr76882

  When you use the **vty-async** global configuration command on a Cisco router that is running Cisco IOS Release 12.0(11) with a virtual template, the second call is not established, but the third call works. There is no workaround.

Wide-Area Networking

- CSCdp66267

  A Cisco 4500 series router reloads with a bus error in nov_fastswitch. There is no workaround.

- CSCdr54259

  A router experiences a software-forced reload with a bus error every 5 to 10 minutes after the **broadcast trigger** command is enabled on a map list associated with an active Frame Relay switched virtual circuit (SVC).

  Workaround: Do not enter the **class** command under the **map-list** global configuration command.

- CSCds34812

  A Cisco router running a LAN emulation client sends a no-src LE_NARP message when it switches over to the standby mode. A no-src LE_NARP message is a LAN emulation version 2 message that is sent to advertise to the other LAN emulation clients that the binding between target-mac address and target-atm address is no longer valid. This message can confuse the Hosts running LAN emulation version 1 client depending on the sequence in which they receive no-src LE_NARP from the standby router and LE_NARP from the active router. This situation results in a temporary loss of connectivity, which will be restored once the client retries the address resolution process. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(13)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(13). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdr57350

  A Cisco router that is running Cisco IOS Release 12.0 might unexpectedly reload while it is performing Simple Network Management Protocol (SNMP) functions related to routing table information (specifically ipRouteNextHop). The reload occurs only in cases where an IP route configuration of the form "ip route <network address> <netmask> 0.0.0.0" exists. There is no workaround.

IBM Connectivity

- CSCdm46549

  Receiving Intermediate Transmission Block (ITB) characters in bisync on some Cisco routers will cause memory corruption and cause a software-forced reload. There is no workaround.

- CSCdr46359

  Frame Relay Access Support (FRAS) boundary access node (BAN) works over the primary connection and switches to the backup connection. However, when it switches to the primary connection from the backup connection, it does not work. There is no workaround.

- CSCdr75061

  A Cisco router might experience a software-forced reload with an error at PC 0x6026107. The decode of the stack is as follows:

  ```
  System was restarted by error - a Software forced crash, PC
  0x60261070[abort(0x60261068)+0x8] Image text-base: 0x60008918[_start(0x60008918)+0x0],
  data-base: 0x60DA0000[etext(0x60d9e4f0)+0x1b10] FP:
  0x6191DF18[etext(0x60d9e4f0)+0xb7fa28], RA: 0x60261070[abort(0x60261068)+0x8] FP:
  0x6191DF18[etext(0x60d9e4f0)+0xb7fa28], RA: 0x6025F890[crashdump(0x6025f7ac)+0xe4] FP:
  0x6191DF30[etext(0x60d9e4f0)+0xb7fa40], RA:
  0x60A42B78[appn_crashdump(0x60a42b60)+0x18] FP:
  0x6191DF48[etext(0x60d9e4f0)+0xb7fa58], RA: 0x60A42004[Pexit(0x60a41f7c)+0x88] FP:
  0x6191E0A0[etext(0x60d9e4f0)+0xb7fbb0], RA: 0x60A3B800[xM_Mget_x(0x60a3b4d0)+0x330]
  FP: 0x6191E1E0[etext(0x60d9e4f0)+0xb7fcf0], RA: 0x60A3AE98[Mget_x(0x60a3ae20)+0x78]
  ```

```
FP: 0 x6191E300[etext(0x60d9e4f0)+0xb7fe10], RA:
0x60A3B898[_MPget_clr(0x60a3b85c)+0x3c] FP: 0x6191E328[etext(0x60d9e4f0)+0xb7fe38],
RA: 0x609E2FC8[xxxtpd01(0x609e2d58)+0x270]
```

There is no workaround.

There may be other symptoms present elsewhere in the network leading up to this reload, such as locates timing out and no new sessions being established.

- CSCdr75809

  A Cisco router running Cisco IOS Release 12.0 with data-link switching (DLSw) configured might reload if the DLSw peers are misconfigured in a way that one DLSw peer is configured for priority and the other end is not. Also, when the router tries to bring up the priority peer, the DLSw peer with no priority might reload.

  Workaround: Fix the configuration so that the DLSw priority peers are properly configured.

- CSCdr83347

  A router running Cisco IOS Release 12.0(9) with bridging and data-link switching (DLSw) processes experiences a software-forced reload at PC 0x60236F0. There is no workaround.

Interfaces and Bridging

- CSCdm84527

  If the input line to a PA-A3 port adapter in a Cisco 7200 or 7500 series router is not functioning properly and the port adapter is experiencing many alarms or errors on the line, link-up messages may appear without link-down messages on the console logs.

  Confirm this occurrence by entering the **show controllers atm** privileged EXEC command. Check the cables and the interface on the other end of the link for problems. There is no workaround.

- CSCdp00618

  A Route Switch Processor (RSP) might reload while unprovisioning a channelized interface under heavy traffic. There is no workaround.

- CSCdp97805

  When a bad transmit packet is generated and sent to the Channelized T3 (CT3) interface, the packet might cause the address of the transmit queue accumulator (txacc) value to not increment correctly for the CT3 interface. In this situation, the output eventually becomes stuck when the txacc value reaches zero.

  Workaround: Configure the CT3 interface with the **tx-queue-limit** *5* interface configuration command to restore the txacc value for the effected CT3 interface.

- CSCdp99133

  A Cisco 7500 series router with VIP2 Versatile Interface Processor boards containing a PA-ATM Enhanced port adapter and a PA-POS port adapter will experience an interface reload and will not be able to send or receive traffic.

  Workaround: Configure these two high-speed PAs on different VIPs.

IP Routing Protocols

- CSCdr27659

  In Cisco IOS Release 12.1 and Release 12.1 T, the IP policy cache is not cleared when you use the **no ip route-cache policy** interface configuration command.

  Workaround: Use the **clear ip cache** [*address-prefix address-mask*] privileged EXEC command for a specific cache.

- CSCdr39819

  A Cisco Catalyst 6000 family switch with a Multilayer Switch Feature Card (MSFC) might reload when the **show ip pim neighbor** EXEC command is issued. There is no workaround.

- CSCdr49658

  A Cisco 3640 router with Cisco IOS Release 12.1(2) reloads with the system returned to ROM by bus error at PC 0x601F9A28, address 0xFFFFFFF9.

  Workaround: Turn off default IP fast-switching if it is on.

- CSCdr49753

  Cisco IOS Network Address Translation (NAT) might stop working if an overload mapping is configured and an extensive File Transfer Protocol (FTP) data session is generated across the NAT router.

  Workaround: Reload the router.

- CSCdr63309

  If you remove the last **redistribute** router configuration command from Open Shortest Path First (OSPF) that used type-1 metric, other routers might not remove the routes from the routing table even though the OSPF database entries are successfully removed.

  Workaround: Keep the router from which you removed the **redistribute** router configuration command as an autonomous system boundary router (ASBR) by removing one redistribution completely and keeping another dummy redistribution.

  Alternate workaround: Do not use the **no redistribute** router configuration command. Flush all the link-state advertisements (LSAs) by using the **redistribute** [**route-map** *foo*] router configuration command. Under **route-map** *foo*, disallow all routes. Enter the **clear ip ospf redist** command. Now you can safely remove the **redistribute** router configuration command completely.

- CSCdr67362

  The hash value used for rendezvous point (RP) selection process in a bootstrap router (BSR) is calculated with a modulo of 2 to the power of 32. This modulo might cause inconsistency in the selected RP address between Cisco and other vendors implementing BSR.

  Workaround: Follow these rules to avoid inconsistency between Cisco routers when upgrading Cisco IOS software:

  If you plan to upgrade routers in your network that use BSR, avoid running Cisco IOS Release 12.0(10)S, Release 12.0(11)S, Release 12.0(11), or Release 12.1(2).

  When upgrading your routers, always upgrade the candidate BSR routers first to a release later than Cisco IOS Release 12.0(10)S, Release 12.0(11)S, Release 12.0(11), or Release 12.1(2). You do not need to upgrade the rest of you network immediately unless you are running the images in CSCdp95116 that might cause the routers to choose the RP on the basis of an incorrect hash value.

- CSCdr73314

  A Cisco router that is running Open Shortest Path First (OSPF) on Cisco IOS Release 12.0(11) does not populate the routing table properly. When redundant paths exist, half of the paths are missing from the routing table. However, the missing networks appear in the OSPF database.

  Workaround: Run a full shortest path first (SPF) by doing **clear ip route *** EXEC command.

- CSCdr76801

  An Address Resolution Protocol (ARP) alias configuration is lost after a Cisco router reloads or after you use the **no shut** command on an interface.

  Workaround: Explicitly reconfigure the arp-alias entries for the IP addresses of the interface after using the **no shut** command.

- CSCds04548

  Open Shortest Path First (OSPF) does not work on unnumbered interfaces.

  Workaround:Enter the **ip address** interface configuration command.

ISO CLNS

- CSCdr59905

  A Cisco router that is running Connectionless Network Service (CLNS) and is redistributing ISO-IGRP (Interior Gateway Routing Protocol) into ISIS might reload if a neighboring ISO-IGRP router sends it a routing update that contains a default prefix router if the prefix route whose next-hop is through “default” is then used for routing packets. There is no workaround.

Miscellaneous

- CSCdp05541

  A system reloads when a crypto map is deleted for a subinterface. There is no workaround.

- CSCdp37597

  A Cisco 7500 series Route Switch Processor (RSP) that is running Cisco IOS image rsp-jsv-mz.112-18 might reload with a segV exception error while performing encryption processing. There is no workaround.

- CSCdp52635

  Voice calls on an AS5300 running with a mix of Regular PRI and NFAS Configuration might fail on dial-peers matching the NFAS Trunks. There is no workaround.

- CSCdp85437

  Routers using Cisco Encryption Technology (CET) may not be able to set up encrypted connections in networks with redundant links between encrypting peers. This may result in crashing the router.

  There is no workaround.

- CSCdp93988

  A Cisco 7200 series router might reload because of memory corruption and exhibit the following error message:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 520 bytes failed fr om 0x60395028, pool
  Processor, alignment 0 -Process= "Pool Manager", ipl= 4, pid= 4 -Traceback= 603C84DC
  603C9F88 60395030 603D4578 603C2C34 603C2C20
  ```

There is no workaround.

- CSCdp95498

  Ciscoview 4.2 might not work properly on a Cisco 7513 router that is running Cisco IOS Release 12.0(9). This situation occurs when slots 0, 2, 5, and 9 are populated with VIP2 Versatile Interface Processors and PA-8T-V35 port adapter cards. CiscoView 4.2 might not show the PA-8T-V35 port adapter on slot 9. Other slots might also report incorrect information. This situation is caused by Simple Network Management Protocol (SNMP) agent, not CiscoView 4.2. The output of the snmpwalk command shows the wrong cardType with a note indicating that indices 19 and 24 are "unknown." There is no workaround.

- CSCdr50614

  An NM-2E2W, NM-1E2W, NM-1E1R2W network module with a BRI WAN interface card (WIC) and a WIC-T1CSU on a Cisco 3600 series router might function incorrectly on rare occasions. When this problem happens, ISDN layer 1 on the BRI WIC is persistently deactivated and the WIC-T1CSU continues to work corrrectly (if no event requires the integrated CSU/DSU to signal the main IOS, in which case it ceases to pass date) except that the **show service-module serial** privileged EXEC command returns an error message.

  Workaround: Power cycle the router.

  Alternate workaround: Reload software.

- CSCdr68325

  A Cisco 7500 series router that is running encryption in Cisco IOS Release 11.2 might experience spurious access and a software-forced reload after displaying the following log messages:

  ```
  Crypto engine 4: sign message using crypto engine: %SYS-2-NOBLOCK: idle with blocking
  disabled -Process= "Crypto SM"
  ```

  There is no workaround.

- CSCdr76238

  The VLAN0 of a Route Switch Module (RSM) participates in Open Shortest Path First (OSPF) election. There is no workaround.

- CSCdr83309

  Cisco Encryption Technology (CET) fails when you try to connect a third peer in a hub and spoke topology and two active connections are already up . When one active connection is dropped, the third peer is able to connect. There is no workaround.

- CSCdr92559

  A new Hot Standby Router Protocol (HSRP) message type introduced in Cisco IOS Release 12.1(3)T causes the STANDBY-3-BADAUTH error message to be displayed periodically. This does not affect the operation of HSRP, and the message can be ignored.

  Workaround: Upgrade to Cisco IOS Release 12.0(13).

Wide-Area Networking

- CSCdr07506

  On a Cisco router, routes on multipoint subinterfaces are not learned within 360 seconds when static map is not configured.

  Workaround: Configure static map using the **frame-relay map** interface configuration command.

- CSCdr16095

  This defect provides ATM Signalling Control Plane Failure Detection through signalling diagnostic MIB objects so the Network Management Station can monitor and take appropriate corrective steps in erroneous situations. There is no workaround.

- CSCdr53700

  You may see the message "%ALIGN-3-SPURIOUS: Spurious memory access ..." when Microsoft callback is being used and a callback fails to complete. The stack trace indicates the alignment error occurred in the dial_if() function, called from dialer_enable_timeout().

  There is no workaround.

- CSCdr77993

  A Cisco 2600 series router running Cisco IOS Release 12.0(11.6) reloads when a call connects with Multilink PPP configured on Dialer Interface. There is no workaround.

- CSCdr87607

  When you load system software to upgrade from any version of the following Cisco IOS releases: 11.1 CC, 11.1 CA, 11.2 P, or 12.0 to any Cisco IOS Release 12.1 or later, the system logging messages for Frame Relay DLCI and subinterface status change are suppressed, regardless of the logging destination (console, buffer, or host).

  Workaround: To resume generating Frame Relay DLCI logging messages, issue the **logging event dlci command**. To resume generating subinterface status messages, issue the **logging event subif** command.

Resolved Caveats—Cisco IOS Release 12.0(12)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(12). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdm91180

  If you use hardware compression and fancy queueing with two simultaneous traffic streams (for example, FTP and Telnet), packets are not compressed. Entering the show compress EXEC command will not provide any useful information. There is no workaround.

- CSCdp31382

  IP Security (IPSec) configured with fast switching works only on serial interfaces and fails on other types of interfaces. There is no workaround.

- CSCdp81754

  A Cisco AS5300 access server reloads with a bus error at PC 0x6022A3C8. This situation occurs during an attempt to telnet to a named-host. There is no workaround.

DECnet

- CSCdr02921

  A Cisco router that is running Cisco IOS Release 12.0(8) might experience an unexpected system reload when you use the **clear decnet accounting** EXEC command or the **no decnet accounting** interface configuration command.

  This situation will only occur if DECnet accounting has been enabled on at least one interface and DECnet traffic is being forwarded by the router at that point in time. This situation is more likely to occur if the following error message has been logged:

  ```
  %SCHED-2-EDISMSCRIT:Critical/high priority process DECnet Input may not dismiss.
  -Process= “DECnet Input”, ipl= 0, pid= 74
  ```

  Workaround: Do not enable DECnet accounting on any interface.

IBM Connectivity

- CSCdm78843

  A Cisco router might reload if there are a large number of Native Client Interface Architecture (NCIA) clients with heavy NCIA traffic because of a watchdog timer. There is no workaround.

- CSCdr41479

  When remote source route bridging (RSRB) is configured on two Cisco 4500 series routers that are connected by an ATM network, and RSRB is configured with an encapsulation type of Fast Sequenced Transport (FST), some frames might not be forwarded. This situation might result in a data-link connection (DLC) session not being established through the RSRB peers.

  Workaround: Either change the RSRB encapsulation from FST to TCP, or configure data-link switching (DLSw) as the transport.

- CSCdr49638

  A Dependent Logical Unit Requester (DLUR) router with High-Performance Routing (HPR) might log the following error messages:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 276 bytes failed from 0x60336D28, pool I/O,
  alignment 32
  ```

  The Systems Network Architecture (SNA) client will not be able to connect to HOST. According to the output of the **show memory** EXEC command, both the processor memory and I/O memory are reduced. There is no workaround.

IP Routing Protocols

- CSCdr11784

  If you configure Protocol Independent Multicast (PIM) or Hot Standby Router Protocol (HSRP) on an ATM-LANE interface, the CPU of the Route Switch Processor (RSP) might reach 99 percent. This situation only occurs when Open Shortest Path First (OSPF) is enabled on more than 12 interfaces in combination with ATM-LANE. This situation does not occur on an RSP that is running Cisco IOS Release 12.0 S or Release 11.2 GS. There is no workaround.

- CSCdr45560

  A Cisco nondesignated router on a multiaccess interface creates state for (S, G) with the Olist populated when receiving a multicast packet. This situation causes a periodic assert every three minutes. There is no workaround.

ISO CLNS

- CSCdm91745

  On Cisco routers, if a DECnet packet is received on an ethernet interface and is converted to a CLNS packet, in the unlikely event that it cannot be routed to its destination, an unexpected reload might occur in ether_extract_addr. There is no workaround.

Miscellaneous

- CSCdp56613

  When fast switching an IP frame that is fewer than 46 bytes in length to an ATM interface, the router always sets the length in the ATM adaptation Layer 5 (AAL5) header to 54 bytes even though the length should be equal to the IP frame length plus the length of the AAL5 header, which is 8 bytes. There is no workaround.

- CSCdr00694

  A Cisco router that is running Cisco IOS Release 12.0(9)S or later releases might experience problems if you attempt to format, delete, or squeeze slot0: immediately after the **show version** command is entered or immediately after the router reloads. This is a flash timing-related issue, and subsequent commands that you enter will not be effected. There is no workaround.

- CSCdr28140

  A Cisco router (800 series through 4700 series) might silently drop large packets. This situation occurs when both Cisco Express Forwarding (CEF) and output rate-limiting are enabled on an interface, and a packet to be switched out of an interface is larger than the maximum transmission unit (MTU).

  Workaround: Disable CEF or disable the Committed Access Rate (CAR) on interfaces that will need to fragment packets.

- CSCdr55357

  A Cisco router that is configured with Multiprotocol over ATM (MPOA) and Cisco Express Forwarding (CEF) might create an ingress cache and an egress cache with the same IP address, and the egress MPOA Client (MPC) address of the ingress cache points to itself. This situation might create a routing loop that causes the router to function improperly. This situation might occur during the route transitions in the network caused by topology changes.

  Workaround: Clear the CEF adjacencies using the **clear adjacency** EXEC command. Clear the corresponding ingress and egress caches using the **clear mpoa client cache** [**ip-address** *ip-address*] EXEC command.

- CSCdr63500

  Configuring a Cisco Route Switch Processor RSP with Multiprotocol over ATM (MPOA) and Cisco Express Forwarding (CEF) might lead to data loss when CEF uses the virtual channel connection (VCC) that was created by MPOA Client for data transfer in the following cases:

  Absence of MPOA client ingress cache

  Absence of the VCC created by MPOA Client

  Workaround: Clear the CEF adjacencies using the **clear adjacency** EXEC command.

Novell IPX, XNS, and Apollo Domain

- CSCdr46313

  In Cisco IOS Release 12.0 and 12.1, but not in earlier releases, a Cisco router that is running Internetwork Packet Exchange-Enhanced Interior Gateway Routing Protocol (IPX-EIGRP) Service Advertising Protocol (SAP) on unstable WAN links might cause IPX EIGRP SAP packets to remain in memory, eventually exhausting processor memory.

  Workaround: Run Routing Information Protocol (RIP)/SAP instead of EIGRP/SAP on the WAN links.

TCP/IP Host-Mode Services

- CSCdr18925

  Remote source-route bridging (RSRB) data is corrupted when you use the **ip tcp path-mtu-discovery** interface configuration command, the IP path changes because of a change in the IP routing metric values, and the largest workable maximum transmission unit (MTU) changes from a larger MTU to a smaller MTU given the path change.

  Workaround: Disable the PATH MTU discovery algorithm by using the **no ip tcp path-mtu-discovery** interface configuration command.

Wide-Area Networking

- CSCdp65239

  The input queue on a Cisco 7500 series router might show 76/75, which can result on the line going down on a High-Speed Serial Interface (HSSI) port adapter even though the VIP console shows that the queue is empty and the line protocol is up. This condition only occurs when PPP encapsulation is enabled.

  Workaround: Move the card to a new slot, change to High-Level Data Link Control (HDLC), or reload the router.

- CSCdr28255

  A Cisco router might reload with the following error when the **frame-relay qos-autosense** and **frame-relay traffic-shaping** interface configuration commands are configured:

  System was restarted by error - an arithmetic exception.

  Workaround: Disable **frame-relay qos-autosense** and configure the shaping parameters manually instead.

- CSCdr32690

  On an access platform, when dialer profiles and virtual profiles are used together with the callback of some vendors, the virtual profile is not applied to the callback call. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(11)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(11). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdp08710

  A Cisco 7200 series router with a compression service adapter (CSA) that is configured with Frame Relay Traffic Shaping (FRTS), and using either Cisco Express Forwarding (CEF) or fast switching will not compress data when the amount of data on the interface is greater than the shaping value. (For example, CSA will stop compression when traffic shaping becomes active.)

  Workaround: Use process switching.

- CSCdp96893

  A Cisco 7500 series router that is configured with a High-Speed Serial Interface (HSSI) port adapter will experience a Virtual Interface Processor (VIP) reload when distributed software compression or hardware compression is configured. When you update the image, the bootloader also needs to be updated, or router will experience the same reload at boot time.

  Workaround: Disable compression or use software compression.

- CSCdr02938

  The Block Serial Tunneling (BSTUN) character set ASCII mode on a Cisco 1600 serial interface does not interoperate with some Binary Synchronous Communication Protocol (Bisync) implementations. Bisync will reject frames that have trailing packet assembler/disassembler (PAD) (0x7F) characters. There is no workaround.

- CSCdr18978

  Number expansion does not work properly. There is no workaround.

IBM Connectivity

- CSCdp60118

  A Cisco router might reload in Tfind_next call because of corrupted memory. There is no workaround.

- CSCdp87156

  If you reload the head router on a Block Serial Tunneling (BSTUN) network, the BSTUN state might stay open on the head router but close on the remote router.

  Workaround: Enter the **no bstun route** command followed by the **bstun route** command to open the tunnel on both sides.

- CSCdp97116

  A Cisco 7500 series router might reload with a bus error at PEfree_ips. There is no workaround.

- CSCdr04949

  A Cisco router might reload when it runs out of processor memory.

  Workaround: Turn off High Performance Routing (HPR).

- CSCdr22737

  The dependent logical unit requester (DLUR) session status remains after you implement INACT on a local Systems Network Architecture (SNA) major node from virtual telecommunications access method (VTAM). There is no workaround.

Interfaces and Bridging

- CSCdk45616

  Distributed switching is not supported for LAN Emulation (LANE) on a Cisco ATM Lite port adapter (PA). There is no workaround.

- CSCdp34500

  A Cisco 2600 router that is configured with a token ring interface or a Cisco 7200 or 7500 series router that is configured with a PA-4R-DTR port adapter token ring interface that is running Advanced Peer-to-Peer Networking (APPN) with Cisco Link Services (CLS)-managed LLC2 logical link control connections might fail host link activation with sense codes 10160007 or 10160022. A router with PA-4R or PA-4R-FDX port adapters is not affected.

  Workaround: Enable source route bridging on the affected token ring interface.

- CSCdp79520

  Under rare conditions, a Cisco router that is running the rsp-jsv56i-mz (56-bit encryption) software image on Cisco IOS Release 12.0(8) might experience a bus error if the box is configured for Data Link Switch over a Token Ring adapter.

  A stack trace decode reveals the following:

```
--> 0x600A5D90:tr_bcast(0x600a5d80)+0x10 --> 0x6026B590:rsp_tx_start(0x6026b148)+0x448
--> 0x601F9EBC:datagram_out(0x601f9664)+0x858 -->
0x607ABDF0:llc_wput(0x607aae2c)+0xfc4 -->
0x60A8FF14:CLSSapUDataStnReq(0x60a8fdcc)+0x148 -->
0x60A8C5F0:CLSSapHandleMsg(0x60a8c4a8)+0x148 -->
0x60A89798:CLSDluSendToSap(0x60a896d0)+0xc8 -->
0x60A90908:CLSWritePut(0x60a90844)+0xc4 --> 0x60ABCF64:fsm_to_disp(0x60abcce0)+0x284
--> 0x60AD09A0:csm_send_to_disp(0x60ad06ac)+0x2f4 -->
0x60AD0658:csm_lan_put(0x60ad010c)+0x54c -->
0x60AD542C:ssp_nonnb_frame_proc(0x60ad4e5c)+0x5d0 -->
0x60AD2244:csm_ssp_handler(0x60ad1928)+0x91c -->
0x60AB8FCC:dlsw_pre_proc_ssp(0x60ab8de4)+0x1e8 -->
0x60AB9460:peer_to_core(0x60ab93f0)+0x70 --> 0x60AA2C58:peer_input(0x60aa283c)+0x41c
--> 0x60AAA694:dlsw_tcpd_readf(0x60aaa274)+0x420
```

  There is no workaround.

IP Routing Protocols

- CSCdm44976

  IP access lists always permit IP fragments. There is no workaround.

- CSCdp67510

  If no interface is specified as part of the **offset-list** router configuration command, a traceback might be generated. There is no workaround.

- CSCdp81134

  A Cisco router that is acting as an area border router (ABR) connected to a stub area might place an Open Shortest Path First (OSPF) external route into its routing table whose outgoing interface is in the stub area. This situation can cause a routing loop because the stub area routers do not know about the external route and will forward packets along their default route, which might be the ABR.

  This problem has been found to occur only when there are 2 paths between the stub area ABR and the autonomous system border router (ASBR) that is originating the external route, where one path is through the stub area and the second is through a nonstub area(s).

  Workaround: Set the link costs within the stub area high enough so that the stub area ABR routers do not see the path to the ASBR as being as good as the path(s) through the nonstub areas.

- CSCdp95116

  In a Protocol Independent Multicast (PIM) Version 2 router configuration, if a hash mask is not configured on a Cisco bootstrap router (BSR), the router takes the first rendezvous point (RP) address from the local RP-mapping cache. The RP-mapping cache is not sorted, so when RPs are added and deleted from the cache, there might be inconsistency through the BSR domain that causes routers to choose different RPs for the same group.

  Workaround: Create a hash mask length of 1 on the BSR router by entering the **ip pim bsr-candidate** *Ethernet1/2 1* global configuration command.

- CSCdr03120

  When you change the Reverse Path Forwarding (RPF) interface for (*,G) and (S,G), the interface that was in the outgoing interface list (O-list) becomes the new RPF interface. At this point, the new RPF interface will be deleted from the O-list which becomes NULL. When the router switches back to the original RPF interface, the O-list remains NULL until the next Internet Group Management Protocol (IGMP) report. While the O-list is NULL, and the original RPF interface has directly connected members, the CONNECTED flags are deleted and the router switches back to the shared tree by sending (S,G,RPT) Join. This situation causes a delay in the convergence time. There is no workaround.

- CSCdr06681

  If there is a link flap somewhere in the network between the area border router (ABR) and an autonomous system boundary router (ASBR), the ABR might not generate a type 4 summary ASBR link-state advertisement (LSA) to other areas after the link is restored. The net effect is that routes being redistributed by the ASBR into Open Shortest Path First (OSPF) will not be installed in the routing tables in the affected areas.

  Workaround: Restart OSPF on the ABR by using the **clear ip ospf proc** command.

  Alternate Workaround: On the ABR, restart OSPF for the affected areas only by removing and restoring the network statements under the **router ospf** global configuration command for the impacted areas.

  Alternate Workaround: For this workaround, perform the action only after the subject ASBR LSA has been removed from the affected areas' database (no longer seen in **show ip ospf database** EXEC command).

  On the affected OSPF routers (that are not seeing the routes and the ASBR LSA) adjacent to the ABR, reestablish adjacencies with the ABR. One way to do this is to temporarily change the hello-interval to some other value. After the adjacency is taken down, change the hello-interval back to the original value to reestablish the adjacency. This action causes the ABR to regenerate and resend the LSAs. On the ABR, create and remove a wrong **router ospf** global configuration command (for example, **router ospf 1234** and **no router ospf 1234)**.

- CSCdr13715

  Due to new RFC 2328, the calculation of summary route costs have changed. This situation might create suboptimal routing, if all of the area border routers (ABRs) are not upgraded to the new code at the same time.

  Workaround: Upgrade all of the ABRs to the new code.

Miscellaneous

- CSCdk34319

  After highly stressing packets through a PA-A3 on a Cisco 7200 series router, if you remove the card and reinsert it to a different slot with a new configuration on the same interface at the new slot, the router might reload with the following error patterns occurring on the console:

  ```
  %SYS-2-LINKED: Bad enqueue of 60DFD980 in queue 60CCFB30 -Process= “<interrupt level>”,
  ipl= 1 -Traceback= 602398F0 601C1370 602000C8 60203958 601C4408 601C81B0
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=14AF, count=0 -Traceback= 601C14FC
  602000C8 60203958 601C4408 601C81B0
  ```

  There is no workaround.

- CSCdm61723

  A reverse telnet to the modem on a Cisco 2600 series router that is running Cisco IOS Release 12.0(5.2)T and that is configured with an NM-8A/S network module interface, does not work. This situation does not occur in earlier Cisco IOS releases. There is no workaround.

- CSCdp19299

  Pings fail with IP Security (IPSec) when you configure fast switching or flow switching. The router exhibits the follow message:

  ```
  %IPFAST-2-PAKSTICK: Corrupted pak header for xxx, flags 0x80
  ```

  Workaround: Use Cisco Express Forwarding (CEF) switching.

- CSCdp54039

  On Cisco routers that are running Cisco IOS Release 12.0(8), IP Security (IPSec) will send in the clear packets that need to be encrypted and fragmented. There is no workaround.

- CSCdp78040

  A Cisco Route Switch Processor (RSP) that is configured with a Multiprotocol over ATM (MPOA) Client might occasionally reload. There is no workaround.

- CSCdp78051

  A Cisco Route Switch Processor (RSP) that is configured with a Multiprotocol over ATM (MPOA) client might have spurious memory access. This situation might degrade MPOA shortcut performance. There is no workaround.

- CSCdp84053

  On a Cisco 2600 series router that is running Cisco IOS Release 12.0(8.1) or later releases, or a Cisco 3640 router that is running Cisco IOS Release 12.0(8.1) or later releases, a serial interface on a Cisco Network Management-8 access server card that is running Block Serial Tunneling (BSTUN) might not come up after a router reload.

  Workaround: Use the **shut** command followed by the **no shut** command, or use the **clear interface** EXEC command to clear the serial interface.

- CSCdp86111

  When Cisco Express Forwarding (CEF) is configured as part of a large configuration (typically with access lists), following boot traffic that is directly addressed to the interfaces of a router might not be received. This condition can be observed on enabled interfaces where IP interfaces appear to be up, but the CEF interfaces are down.

  Workaround: Perform one of the following steps. Boot without CEF enabled. Disable and then re-enable CEF. Enter the **no shutdown** command on each of the interfaces that are affected.

- CSCdp89389

  A Cisco 3600 or 2600 series router with a NM-8A/S or NM-4A/S interface that has a **physical-layer async** command configured on the serial interface might see junk characters on the serial line during bootup time. No other functionality is affected. There is no workaround.

- CSCdp95036

  A Cisco Versatile Interface Processor (VIP) that is configured with Cisco Encryption Technology (CET) might not initiate a new crypto connection. The VIP will respond to a connection request from the remote end. However, if the remote end is also a VIP, the crypto connection might never be initiated, because both VIP routers will wait on a connection request. There is no workaround.

- CSCdp96890

  On a Cisco 7500 series router, if Cisco Express Forwarding (CEF) is enabled, Web Cache Control Protocol (WCCP) or one or more tunnel interface is configured, and packets that are redirected by WCCP or transmitted over a tunnel arrive over an Inter-Switch Link (ISL) interface, then packets terminating at the router that arrive over the same ISL interface might be dropped. For example, pinging to or from the router might show a 10 to 30 percent packet loss. There is no workaround.

- CSCdp97482

  On a Cisco router with port channel interfaces with Inter-Switch Link/Token Ring Inter-Switch Link (ISL/TRISL) encapsulation, any changes on the encapsulation might cause a Cisco bus (cbus) restart. The system returns to normal operation after the cbus restart. There is no workaround.

- CSCdr00015

  When a remote Cisco 2600 series router or a Cisco 3600 series router goes down, the BRI line protocol that is configured as “leased line 128K” might not go down properly. The router repeatedly displays the following message while the remote site is down:

  ```
  %LINK-3-UPDOWN: Interface BRI1/0, changed state to up” while the remote site has been down.
  ```

  This situation occurs when you use a NM-4BRI network module or a NM-8BRI network module and the router is configured with High-Level Data Link Control (HDLC) encapsulation. There is no workaround.

- CSCdr03335

  On a Cisco router, 50 percent of pings might fail to receive replies when you use the **ip cef** global configuration command so the router probably drops packets frequently. There is no workaround.

- CSCdr04916

  Hot Standby Router Protocol (HSRP) tracking does not work properly. When an interface is tracked, it goes into standby state. When it comes out of standby state, the information is not updated so the tracking interface gets stuck in standby state. There is no workaround.

- CSCdr09895

  Under heavy traffic, a PA-A3 port adapter might experience a SAR0 reload. If this condition occurs on a Cisco 7200 series router, you must reload the router to recover normal operation. On a Cisco 7500 series RSP, this situation might result in commands from the RSP to the port adapter failing, but the port adapter should be able to recover without a router reload. There is no workaround.

- CSCdr23563

  A Cisco Route Switch Processor (RSP) that is configured with multiprotocol over ATM (MPOA) clients might take more packets than usual (approximately 500) to transfer the data through MPOA shortcut. There is no workaround.

- CSCdr25598

  A Cisco Route Switch Processor (RSP) might reload when Generic Traffic Shaping (GTS) is enabled on an interface. This situation only affects RSPs. The RSP will reload when you configure the GTS with the **traffic-shape group** interface configuration command with an access list that has a deny statement in it. There is no workaround.

Wide-Area Networking

- CSCdp57518

  In Cisco IOS Release12.0, if you use the **ppp pap sent-username** *username* **password** *password* interface configuration command on a dialer profile, this command must also be added to the physical interface. There is no workaround.

- CSCdp79091

  With X.25 over TCP (XOT), when there are many IP addresses in the X.25 route command and the first IP address is unreacheable, a Cisco router will take the next IP address. The default X.25 parameters are then used instead of the ones configured on the X.25 interface which causes the X.25 public switch to clear the call. There is no workaround.

- CSCdp99013

  When Frame Relay traffic shaping is configured and either custom queueing or priority queueing is enabled at the virtual circuit (VC) level, an alignment error might occur. The error occurs when the priority/custom queue list checks User Datagram Protocol (UDP) packets and the current packet is a UDP packet that is queued because of traffic shaping. There is no workaround.

- CSCdr28255

  A Cisco router might reload with the following error when the **frame-relay qos-autosense** and **frame-relay traffic-shaping** interface configuration commands are configured:

  ```
  System was restarted by error - an arithmetic exception.
  ```

  Workaround: Disable **frame-relay qos-autosense** and configure the shaping parameters manually instead.

Resolved Caveats—Cisco IOS Release 12.0(10)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(10). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdm81049

  If a serial interface is frequently flapping, the router might pause indefinitely with a stack trace indicating that it is in usecdelay() as a result of cbus_mci_serial_reset() being called while at interrupt level. This situation rarely occurs.

  Workaround: Enter the **shutdown** interface configuration command on the serial interface that is flapping.

- CSCdp28929

  A Cisco router or access server might reload when a reference is made to a teletype (TTY)/Telnet session that has been externally ended. There is no workaround.

- CSCdp32242

  A Cisco 7200 series router that is running PPP stack hardware compression with a compression service adapter (CSA) might reload because of a memory leak. This situation occurs when a PA-MC-T1 port adapter is used. It can also occur when a multichannel E3 PA port adapter is used.

  Workaround: If the CPU can handle the load, enter the **compress** {**predictor** | **stac** [**csa** *slot* | **software**]} interface configuration command.

- CSCdp53468

  You might not be able to change the size of priority queues in priority queueing with virtual template interfaces on a Cisco 3640 router that is running Cisco IOS Release 12.0(8) or Cisco IOS Release 12.0(7). There is no workaround.

- CSCdp57305

  A Cisco 7200 series router that is running Cisco IOS Release 12.0(7) might reload because of a bus error or pause indefinitely when FRF.9 payload compression is enabled with a hardware compression adapter and Frame Relay Traffic Shaping has already been configured on the serial interface.

  Workaround: Use FRF.9 software compression.

- CSCdp60260

  A Cisco router might reload when hardware compression is configured in conjunction with Generic Traffic Shaping and Fancy Queueing on a compression service adapter (CSA) at the main interface. This situation only occurs when all 3 features are configured.

  Workaround: Use software compression.

- CSCdp67197

  A Cisco 2610 router that is running Cisco IOS Release 11.3(6)T might experience leaking memory because of IP Simple Network Management Protocol (SNMP). There is no workaround.

DECnet

- CSCdp50978

  A Cisco router might reload if it pings a DECnet address across an ISDN BRI connection. Pinging IP continues to work, as does DECnet routing. There is no workaround.

IBM Connectivity

- CSCdm66552

  A Cisco 2500 series router might suddenly stop receiving or not forward packet frames while transferring files over data-link switching plus (DLSw+) link using Fast Sequenced Transport (FST) encapsulation. This situation causes the NetBios session to disconnect. There is no workaround.

- CSCdp09939

  A Cisco router might experience a bus error as a result of a timing error. There is no workaround.

- CSCdp43233

  A Cisco 7500 series router that is running a Cisco IOS release higher than the Cisco IOS Release 12.0(3c) might experience a situation where attached Network Basic Input/Output System (NetBIOS) PCs are not reaching the Ethernet-attached NetBIOS server. When this situation occurs, the router sends an incorrect LAN Emulation Address Resolution Protocol (LE_ARP) request, and is unable to resolve the route descriptor for the local LANE cloud and the Token Ring behind the Token Ring switch. A Logical Link Control, type 2 (llc2) frame out of the data-link switching (DLSw) cloud directed to the PC will trigger a LANE LE_ARP lookup on the router for the wrong route descriptor. As a result, the LANE data direct virtual channel connection (VCC) is only used in one direction from the Token Ring switch to NetBIOS PCs, and the NetBIOS connection pauses indefinitely. There is no workaround.

- CSCdp59004

  A Cisco router that is running Advanced Peer-to-Peer Networking (APPN) with High-Performance Routing (HPR) enabled might leak some processor memory when establishing Routing Table Protocol (RTP) connections. These leaks may be seen in cell pools 0, 1, and 2 of APPN Memory Partition 0. There is no workaround.

- CSCdp63998

  A Cisco router that is running Advanced Peer-to-Peer Networking (APPN) might reload after the operator enters the **show appn dlur-pu host-pu** command. There is no workaround.

- CSCdp81656

  A Cisco router that is running Advanced Peer-to-Peer Networking (APPN) High-Performance Routing (HPR) might reload when it receives a Bind Route Request Unit. There is no workaround.

- CSCdp83343

  A Cisco Advanced Peer-to-Peer Networking (APPN) router might reload because of a bus error while attempting to allocate an input/output (I/O) memory buffer. The router exhibits the following error message:

  ```
  Memory allocation of 788 bytes failed from 0x602BE4C0, pool I/O, alignment 32 -Process=
  “cswebtsk”, ipl= 4, pid= 67
  ```

  There is no workaround.

Interfaces and Bridging

- CSCdp40908

  A Cisco PA-A1 port adapter does not automatically switch to the internal clock during LOS (Loss of Signal) condition. There is no workaround.

- CSCdp40929

  A Cisco PA-A1 port adapter does not detect the Loss of Cell Alignment (LOCA) error. There is no workaround.

- CSCdp51752

  In Cisco 7100 and 7200 series routers, transparent bridging using the PA-DTR Token Ring Port Adapter does not operate properly. The **show bridge** command fails to indicate any of the end-stations in the bridge table.

  Workaround: On the Cisco 7200 series routers, use alternative token ring port adapters. There are no known workarounds for the Cisco 7100 series routers.

IP Routing Protocols

- CSCdm80672

  A Cisco router may experience a bus error and reload when you enter the **ip accounting output-packets** command. There is no workaround.

- CSCdp30454

  The dataless header register does not work properly in Cisco IOS Release 12.0(7)S. There is no workaround.

- CSCdp49682

  A Cisco 827 router might reload or experience spurious access in iprouting_destination_valid. The spurious access is caused by reading an invalid location, so memory is not corrupted. There is no workaround.

- CSCdp68820

  Sources of multicast packets that send at a low frequency might have their (S,G) expire in the first-hop designated router (DR). The corresponding (S,G) might also expire in the rendezvous point (RP).

  If the (S,G) state is later created from a Protocol Independent Multicast (PIM) Join packet from downstream, then the register flag is not set for this (S,G) in this router. If a packet is then received from the source, the register packet will not be sent to the RP so the A-flag for the (S,G) will not be set in the RP, which would prevent the subject source from being advertised to the Multicast Source Discovery Protocol (MSDP) peers. There is no workaround.

- CSCdp72071

  When the Protocol Independent Multicast (PIM) designated router (DR) changes, the F flag is not changed. This situation might then cause header registers either not to be sent to the Route Processor (RP) or to be duplicated.

  Workaround: If the router is configured for multicast and the group is sparse mode, use the **clear ip mroute** {*s, g*} EXEC command to fix the F flag.

- CSCdp72137

  When the Incoming Interface List (IIL) changes for a (S,G) state, the F flag is not updated. This situation might cause registers to be sent for sources that are not directly connected anymore. There is no workaround.

- CSCdp99619

  A Cisco RSP4 Route Switch Processor might reload if the managed timer does not work properly. This situation rarely occurs. There is no workaround.

ISO CLNS

- CSCdm89814

  The **redistribute static** command can apply in either the router Intermediate System-to-Intermediate System (IS-IS) context or the router International Organization for Standardization (ISO) Interior Gateway Routing Protocol (IGRP) context. It is possible to differentiate between IP and Connectionless Network Service (CLNS) static routes in router IS-IS, but impossible to differentiate between IP and CLNS static routes in router ISO-IGRP that also automatically append CLNS to the **redistribute static** command.

  Workaround: Upgrade to Cisco IOS Release 12.0(10).

- CSCdp39702

  If a Connectionless Network Service (CLNS) neighbor has multiple associated area addresses, then a Terminal Identifier Address Resolution Protocol addresses, then a Target Identifier Address Resolution Protocol resolve request will automatically choose the first entry. If the first entry is in the process of being replaced by the second area, then the Target Identifier Address Resolution Protocol request will fail.

  Workaround: Clear the CLNS cache.

Miscellaneous

- CSCdk64756

  A Dynamic Host Configuration Protocol (DHCP) proxy agent on a Cisco router assigns the same IP address to users that are on different ports but have the same username.

  Workaround: Assign unique usernames.

- CSCdm70419

  A Cisco router might reload because of a memory corruption. There is no workaround.

- CSCdm85458

  A Cisco router might reload if traffic shaping is configured with committed information rate (CIR) within a range of 1 to 999 bps.

  Workaround: Configure CIR above 1000 bps.

- CSCdp08508

  A Cisco 4500 series router might slow down or pause indefinitely if you configure a mac-forward filter over transparent bridging on a Token Ring interface. There is no workaround.

- CSCdp42529

  A Cisco 7200VXR router might experience a situation where switched virtual circuits (SVCs) are disconnected intermittently and then recovered after 7 to 20 hours. There is no workaround.

- CSCdp43778

  If you configure a subinterface on a Cisco 2600 series router for Operation, Administration, and Maintenance (OAM), and the permanent virtual circuit (PVC) bounces, the PVC and the interface will not come back up unless you enter the **shutdown** command followed by the **no shutdown** command on the interface. This situation does not occur if the PVC is configured without OAM. There is no workaround.

- CSCdp47676

  The **show interface display** EXEC command might show that a Cisco 2-port High-Speed Serial Interface (HSSI) or a Cisco PA-2T3 port adapter is experiencing abnormal transmit underruns on some Versatile Interface Processors (VIPs) with fast protocol control information (PCI) transactions. There is no workaround.

- CSCdp54245

  Multiprotocol over ATM (MPOA) shortcuts might not check for the frame sizes being sent on them. If the frame size exceeds the maximum transmission unit (MTU) size of the egress Multiprotocol over ATM Client (MPC), egress MPC drops the packet, resulting in the loss of connectivity.

  Workaround: Configure matching MTUs on either side of shortcuts (for example, all LAN Emulation Clients (LECs) that are served by ingress and egress MPCs should have the same MTU). If MTUs cannot be altered, then do not configure MPOA on both sides.

- CSCdp57307

  A Cisco Catalyst 5000 might treat the link between the physical interface and the port channel interface as a multidrop link when the mac address of members of a port channel is different from the mac address of the port channel itself. This situation has been fixed in Cisco IOS Release 2.2a.

  Workaround: Delete the members of the port channel and then add then add them back in.

- CSCdp58142

  A Route Switch Processor (RSP) with an interface configured with IP Security (IPSec) crypto map and the switching mode is Cisco Express Forwarding (CEF), the RSP might reload trying to decrypt an IPSec packet. This situation is only seen when CEF switching is on. There is no workaround.

- CSCdp58947

  If the service compress configuration is enabled, entering the **show startup-config** configuration command or the **show config** configuration command will result in a memory leak. There is no workaround.

- CSCdp60273

  When performing tag imposition on a packet that must be fragmented, datagram_done will exhibit a bad reference count error and a traceback message. There is no workaround.

- CSCdp62791

  A Cisco 7200 series router that is running ATM LAN Emulation (LANE) with a PA-A3 port adapter might reload if a packet with invalid encapsulation is sent to the port adapter. There is no workaround.

- CSCdp66962

  If you copy a file through SNMP using TFTP to a flash file system, when the space left on the flash is less than the size of the file you will receive a ciscoFlashCopyStatus of copyOperationSuccess message even though the file was not copied.

  Workaround: Perform the same function through the command-line interface (CLI).

- CSCdp67615

  You cannot use SNMP to partition the flash.

  Workaround: Partition the flash through the command-line interface (CLI).

- CSCdp67643

  On a Cisco router that is running Cisco IOS Release 12.0, a Cisco Encryption Technology (CET) encrypted packet coming in while the router is restarting might prevent encryption from working on that interface for 15 minutes.

  When this situation occurs, the **show crypto map** privileged EXEC command will **show the Connection** ID as BAD, and the connection will not be listed by either the show crypto cisco connections privileged EXEC command or the **show crypto engine connections active** privileged EXEC command. There is no workaround.

- CSCdp69767

  A Cisco router might reload with a bus error if you choose “Clickstart” in the HTML management interface. There is no workaround.

- CSCdp72579

  When a Route Switch Module (RSM) with a large compressed configuration is booted, the RSM might not be considered online by the Supervisor engine.

  Workaround: Boot the RSM without the configuration and use the **copy tftp running-config** command.

- CSCdp76970

  Traffic shaping might cause a Cisco 3640 router to reload under the following conditions:

  – The output queue is first-in, first-out (FIFO).

  – The output queue is congested.

  – The packet matches a shape structure but need not need delayed.

  There is no workaround.

- CSCdp78056

  A Cisco router that is running a Multiprotocol over ATM (MPOA) server might reload if you shut down a neighboring interface that is running a MPOA client (MPC). There is no workaround.

- CSCdp80948

  A Cisco PA-A3 port adapter occasionally exceeds configured peak cell rate (PCR) limits for available bit rate (ABR) and unspecified bit rate (UBR) traffic classes. There is no workaround.

- CSCdp82808

  The Local Management Interface (LMI) is not functioning properly on Cisco routers that are running Cisco IOS Release 12.0(7)T. This situation occurs only with Quad Integrated Communications Controller (QUICC) WAN interface cards (WICs) and not with network modules (NMs). There is no workaround.

- CSCdp84206

  Distributed Cisco Express Forwarding (dCEF) packets with Multiprotocol Label Switching (MPLS) labels that require fragmentation and labeled output and are received on an ATM Lite MPLS subinterface will be dropped.

  Workaround: Disable dCEF on the ATM Lite MPLS interface.

TN3270

- CSCdp50276

  A TN3270 client on a Cisco access server might erroneously leave the keyboard in a locked state causing all keyboard input to be rejected until you press the master_reset keypress. This situation occurs when an application sends write-structured field commands with the keyboard-restore indicator on the associated write-control character. There is no workaround.

Wide-Area Networking

- CSCdp05882

  A Cisco 7200 VXR router might reload with a bus error because the packet-by-packet compression code is being passed packets that contain particles. There is no workaround.

- CSCdp35206

  A Cisco 7200 series router that is running Cisco IOS Release 12.0(7) might reload with a bus error at PC 0x60584578, address 0xD0D0D51. There is no workaround.

- CSCdp40411

  The **frame-relay de-group** *1 local-dlci* interface configuration command might disappear from the running configuration and stop working for the referenced data-link connection identifier (DLCI) if you configure the **frame-relay inverse-arp** interface configuration command and the corresponding permanent virtual connection (PVC) status changes to Inactive or Deleted.

  Workaround: Use the static **frame-relay map** interface configuration command and reference the same DLCI that is used for the **frame-relay de-group** *1 local-dlci* interface configuration command.

- CSCdp41653

  A Cisco router that is running Cisco IOS Release 12.0 or later releases might reload because of a bus error at the symbol dialer_clear_map. There is no workaround.

- CSCdp51357

  When X.25 over TCP (XOT) connects X.25 links that are configured for module 128, the packet assembler/disassembler (PAD) session will pause indefinitely. In this situation, entering the **show x25 vc** EXEC command will return a “Window is closed” message. There is no workaround.

- CSCdp59874

  Timer data structures used by the dialer component might become corrupted. The corruption might occur because of operator-initiated actions that involve the removal of the dialer function on an interface. Examples of these actions would be configuring leased-line BRI, or entering the **no dialer in-band** interface configuration command. The symptom might not occur for days or weeks after the operator action that caused it. Due to this condition, these actions should be avoided. There is no workaround.

- CSCdp60088

  On a Cisco router with dialer profiles, dialer load-threshold, and no multilink, an overload call might not be done even though the load threshold is exceeded. This situation occurs when an incoming call is received with a particular caller ID but there is no dialer string configured with the same phone number.

  Workaround: Initiate first and overload calls from the same router.

- CSCdp60104

  A Cisco router that is running Cisco IOS Release 12.0(8) and is configured with a LAN Extender (LEX) interface might display any of the following error messages:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=Lex0
  -Process= “RIP Send”, ipl= 0, pid= 73
  -Traceback= 1A2006 66872 1A697A 22F1E4 22E924 22EAC0 380A36
  %LINK-2-INTVULN:In critical region with interrupt level=0, intfc=Lex0
  -Process= “IP Input”, ipl= 0, pid= 12
  -Traceback= 1A2006 66872 1A697A 22F1E4 224EAA 2257E0 224902 224A5C 224B80
  %LINK-2-INTVULN:In critical region with interrupt level=0, intfc=Lex0
  -Process= “ARP Input”, ipl= 0, pid= 7
  -Traceback= 1A2006 66872 1A697A 1FE4AC 2398C4 239E80 1FE6D
  ```

  There is no workaround.

- CSCdp63026

  A Cisco router will exhibit traceback messages when the router sends Inverse Address Resolution Protocol (ARP) messages for protocols like Novell, DECnet, and XNS. This situation will not affect router operation. There is no workaround.

- CSCdp65204

  When using dialer profiles, the dialer state could get stuck in the call pending state. In this situation, outgoing ISDN calls can no longer be initiated. There is no workaround.

- CSCdp65743

  Under certain conditions, the **frame-relay inverse-arp** command does not function properly for IPX, Novell, DECnet, and VINES for multipoint interfaces. This situation is more likely to occur when IP is running on the interface.

  Workaround: Create a static map for IPX, DECnet, and other protocols by entering the **frame-relay** *map* interface configuration command, or change the interface from multipoint to point-to-point.

- CSCdp86348

  A Cisco 7500 series router that is running Cisco IOS Releases 11.1(31.1)CC, 12.0(9.1), 12.0(8.6)S1, 12.0(9)S, 12.1(0.8), and 12.1(0.8)T with a PA-A3 port adapter will not send Operation, Administration, and Maintenance (OAM) cells. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(9)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(9). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdm55275

  If an NM-AM modem is set to mark, space, or even parity, the **modem autoconfigure type** line configuration command will not function properly.

Workaround: Use the **script startup** line configuration command and the **script reset** line configuration command.

Basic System Services

- CSCdm20829

  If you enter the **show interfaces** [*type number*] [*first*] [*last*] [**accounting**] EXEC command on a Cisco router that is running Cisco IOS Release 12.0(3)T, the accounting records are updated only when the first system interface is sampled, and all interfaces share the accounting record of the first interface. There is no workaround.

- CSCdm67579

  A Cisco router might stop responding to Simple Network Management Protocol (SNMP) queries. This situation occurs when the number of SNMP request packets to be processed at the same time is high. There is no workaround.

- CSCdm88410

  A Cisco router might reload when you enter the **write memory** EXEC command at the router prompt. This happens during nonvolatile generation (nvgen) of the **line** global configuration command. There is no workaround.

- CSCdp08710

  A Cisco 7200 series router with a compression service adapter (CSA) that is configured with Frame Relay Traffic Shaping (FRTS), and using either Cisco Express Forwarding (CEF) or fast switching will not compress data when the amount of data on the interface is greater than the shaping value (for example, CSA will stop compression when traffic shaping becomes active).

  Workaround: Use process switching.

- CSCdp16189

  Configuring trigger authentication by entering the **ip trigger-authentication** interface configuration command might cause a memory leak. There is no workaround.

- CSCdp60260

  A Cisco router might reload when hardware compression is configured in conjunction with Generic Traffic Shaping and Fancy Queueing on a compression service adapter (CSA) at the main interface. This situation only occurs when all 3 features are configured.

  Workaround: Use software compression.

DECnet

- CSCdp05189

  If you configure a Cisco router using the **decnet routing-timer** *seconds* interface configuration command, the router might create a DECnet in-routing filter access list number after you reload the router. The access list number will be the same as the time in seconds specified in the **decnet routing-timer** *seconds* interface configuration command, and might be invalid. There is no workaround.

- CSCdp21639

  If a Cisco router is running a release earlier than Cisco IOS Release 11.3 and is using the DECnet Phase IV routing protocol, the DECnet network might experience loops or the incorrect selection of routes for periods of time up the value entered with the **decnet routing-timer** interface

configuration command. When a network link goes up or down, one of the routers attached to that link might start sending DECnet traffic down the wrong route. You can enter the **show decnet traffic** EXEC command to show the number of messages that have been discarded with the "too many visits" count. If you enter the **show decnet route** configuration command, you can check the routes selected by the router.

Workaround: Reduce the time in the **decnet routing-timer** *seconds* interface configuration command to reduce the time taken for the network to converge.

IBM Connectivity

- CSCdm77914

  During a rare timing window when the multiple downstream devices are simultaneously deactivated, the Advanced Peer-to-Peer Networking (APPN) router might cause the TP that processes the encapsulated messages received on the conloser DLUR/Dependent LU Server (DLUS) pipe session to pause indefinitely. Once the TP is paused, the DLUR may have some DLUR-PUs and DLUR-LUs that appear to be in a permanently stopped state. The corresponding virtual telecommunications access method (VTAM) resources remain in PDACP or PUSB1 states.

  Workaround: Restart the APPN subsystem on the router.

- CSCdm78005

  A Cisco 4500 router might experience memory alignment errors in Advanced Peer-to-Peer Networking (APPN). There is no workaround.

- CSCdm78880

  A Cisco 4700 router that is configured for data-link switching (DLSw) with Dependent LU Requester (DLUR) and Advanced Peer-to-Peer Networking (APPN) might reload after you issue the **show version** command because of an SegV exception. There is no workaround.

- CSCdp09919

  Remote source-route bridging (RSRB) might change frame types. This situation occurs on Cisco routers that are running RSRB where one side of the RSRB is running any Cisco IOS release prior to Cisco IOS Release 12.0 and the other side is running Cisco IOS Release 12.0. The frame that is moving along the source-route translational bridge (SR/TLB) and the RSRB bridge might change from an Ethernet Type II frame to an IEEE802.3 Ethernet frame.

  Workaround: Configure the 90-compatible option by entering the **source-bridge transparent** *ring-group seudo-ring bridge-number tb-group* [*90-compatible*] global configuration command.

- CSCdp09939

  A Cisco router might reload because of a bus error. There is no workaround.

- CSCdp23809

  A Cisco router that is running Block Serial Tunneling (BSTUN) might experience an input queue wedge. Reloading the router will temporarily fix the situation. There is no workaround.

- CSCdp24741

  A Cisco router that is configured for Advanced Peer-to-Peer Networking (APPN) might experience 80 percent to 90 percent CPU utilization by the lrp00 process. There is no workaround.

- CSCdp53919

  Hundreds of alignment corrections on bridging processes might cause a Cisco router (including console access) to pause indefinitely. There is no workaround.

- CSCdp63021

  A Cisco router might reload through the watchdog timer because Topology and Routing Services (TRS) is looping on a zero length cv46 subvector in unmap_cv46. There is no workaround.

Interfaces and Bridging

- CSCdm74213

  A Cisco PA-A1 is subject to rx packets with bad aal5_length field. If the erroneous length is too small, it might corrupt memory and cause the router to reload. There is no workaround.

- CSCdp15196

  A Cisco 7507 router that is running Cisco IOS Release 12.0(4)T might not return the correct results if there is a change in the hold-queue value in any of the serial interfaces of a PA-8T port adapter in a VIP2 motherboard. Although the size of the output queue seems to change after you enter the **hold-queue out** interface configuration command, there is no real change. There is no workaround.

- CSCdp36862

  A Cisco 7200 series router with a PA-4R port adapter might accept a packet with an invalid frame check sequence (FCS) and pass it on to remote source-route bridging (RSRB). This situation does not occur in the PA-4R-DTR port adapter. There is no workaround.

IP Routing Protocols

- CSCdk81576

  When network statements are removed from the Open Shortest Path First (OSPF) configuration in a router, there is no check executed for overlapping networks, which results in OSPF being disabled on the corresponding interfaces.

  Workaround: Remove the overlapping network statement, and then reinsert it.

- CSCdm54513

  If there is a component route in the routing table that has exactly the same network and mask pair as the summary route, OSPF might delete and later reissue the external summary routes.

  Workaround: Perform a redistribution by entering the **route-map** global configuration command with a deny statement in the access list.

- CSCdm75717

  Internal Border Gateway Protocol (IBGP) routes cannot be redistributed to other protocols. There is no workaround.

- CSCdp03960

  A Cisco 7200 series router that has not been configured might fail to receive Open Shortest Path First (OSPF) route updates from a neighbor router through an ATM LAN emulation (LANE) interface when a script tries to clean and configure the Cisco 7200 series router. This situation does not occur on a router that has already been configured.

  Workaround: Reload the router, or enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdp05306

  After a link flap, the summary route might not appear in the routing table even though it appears in the OSPF topology table.

  Workaround: Restart the OSPF process, or reload the router.

- CSCdp21551

  If you have an Open Shortest Path First (OSPF) external route and a floating static route (as backup for the external route) with the nexthop interface OSPF enabled, and if there is a flap in external route, floating static will be installed in the routing table. The floating static route will not get replaced by the external route, even when the external route comes back up.

  Workaround: Enter the **clear ip route** {*network* [*mask*]|*} EXEC command.

- CSCdp27183

  A Resource Reservation Protocol (RSVP) message will be dropped if the flags or reserved fields in the common header are not set to zero. In this situation, you will not be able to operate within implementations that use these fields for new features. There is no workaround.

- CSCdp30909

  When you are configuring policy routing on a rotary group leader, entering the **no ip policy route-map** *map-tag* interface configuration command on a group-async rotary group member or several physical interface rotary group members might cause the router to reload with a SYS-2-FREEFREE error message. There is no workaround.

- CSCdp39166

  A Cisco router might reload if certain IP packets addressed to a multicast destination with an invalid IP header are received.

  On a Route Switch Processor (RSP), this situation often shows up as a bus error reload with RSP-specific code and ipmulticast_les_fastswitch on stack trace at address=0x58200000.

  This situation might also show up as a generic memory corruption reload on an RSP or on other nonparticle-based platforms. This situation does not exist in Cisco IOS Release 11.1CC and Cisco IOS Release 11.2.

  Workaround: Disable multicast fast switching on all interfaces by entering the **no ip mroute-cache** interface configuration command.

- CSCdp39947

  Protocol Independent Multicast (PIM)v2 Candidate Rendezvous Point (RP) advertisement packets are discarded by a router if the packets were sent by that route.This breaks the Candidate-RP and bootstrap router (BSR) mechanism in PIMv2.

  Workaround: Only configure a Candidate-RP in routers that are not BSR.

Miscellaneous

- CSCdk51490

  A crypto Access Control List (ACL) with a DENY ACE that specifies a TCP or User Datagram Protocol (UDP) port might cause fragments to be dropped.

  Workaround: Arrange the crypto ACLs to have permits only when specifying ports. For example, instead of having:

  ```
  access-list 101 deny udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255 eq 19 access-list 101 deny udp 200.200.20.0 0.0.0.255 eq 19 200.200.30.0 0.0.0.255 access-list 101 permit udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255
  ```

have:

```
access-list 101 permit udp 200.200.20.0 0.0.0.255 ne 19 200.200.30.0 0.0.0.255 ne 19
access-list 101 deny udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255 eq 19 access-list
101 deny udp 200.200.20.0 0.0.0.255 eq 19 200.200.30.0 0.0.0.255
```

- CSCdm36742

  Formatting boot flash memory on a Cisco 7100 series router might disable access to boot flash memory. This situation occurs with crypto images in Cisco IOS Release 12.0(5)XE, Cisco IOS Release 12.0(5)XE1, and Cisco IOS Release 12.0(5)XE2, and the situation might occur with some noncrypto images.

  Workaround: Format Flash with a working image, or do not format Flash.

- CSCdm70036

  Context-based Access Control (CBAC) code might reject the alerting messages that arrive before the connect message that carries the port information for the return data stream. The connect message is processed, but the alerting message needs to be processed first for the data stream to be received properly. There is no workaround.

- CSCdm79157

  Cisco Encryption Technology (CET) might not function correctly when configured on a Cisco router with generic routing encapsulation (GRE) tunnel. There is no workaround.

- CSCdm82594

  Some internal registers might not correctly update when the link goes down.

  Workaround: Upgrade to Cisco IOS Release 12.0(7)T.

- CSCdm90466

  If there is a large network delay and Asynchronous Serial Protocol (ASP) does not support local acknowledgements (ACKs), you need to increase the poll interval on the end device to accommodate the delay. There is no workaround.

- CSCdp05107

  Permanent virtual circuits (PVCs) might not transmit if the configuration for the PVC is changed while the outbound rate on that PVC exceeds sustainable cell rate (SCR).

  Workaround: Enter the **clear interface** *ATM slot/port* EXEC command when this situation occurs.

- CSCdp07473

  A Cisco 7200 series router might reload and display the following error message:

  ```
  %SCHED-2-WATCH: Attempt to enqueue uninitialized watched queue (address 0).
  -Process= “<interrupt level>”, ipl= 1, pid= 2
  -Traceback= 6036BE38 6033C5B4 60258F94 6026F794 603A846C 60266368 6026B988
  ```

  There is no workaround.

- CSCdp07476

  When you enable bridging on a Fast EtherChannel (FEC), the host functionality might not work properly, but bridging functionality is not affected. There is no workaround.

- CSCdp16515

  A Cisco router will reload if IP Security (IPSec) is enabled with fast switching on links that use PPP encapsulation with PPP compression. There is no workaround.

- CSCdp17334

  The second port on a Cisco router with a PA-2T3 port adapter and a PA-2E3 port adapter will not come up if the first port is in a shutdown state.

  Workaround: Enter the **no shutdown** interface configuration command on the first port.

- CSCdp24644

  If devices that can share the same IP address at different times are connected behind an MPC, some Multiprotocol over ATM (MPOA) shortcuts might not be valid after they switch over the IP address. There is no workaround.

- CSCdp24671

  If you have two Cisco switches connected on Gigabit Ethernet Inter-Switch Link (ISL) trunk using SVM 1/1 and with Hot Standby Router Protocol (HSRP) configured on a Gigabit Ethernet port channel with ISL encapsulation in a Cisco switching module, then the module might reload when the HSRP group 255 becomes active. This situation can also occur with dot1q(802.1q) trunking. There is no workaround.

- CSCdp31471

  The Available Bit Rate (ABR) feature on the PA-A3 port adapter is not functioning properly. The PA-A3 driver can send and receive forward resource management (FRM) cells, but cannot transmit backward resource management (BRM). There is no workaround.

- CSCdp33777

  A Cisco router might experience a SIGTRAP exception error and reload. There is no workaround.

- CSCdp36078

  Cisco Lock and Key idle timers will not be reset when there are packets that match the dynamic Access Control Lists (ACLs) created by Lock and Key. There is no workaround.

- CSCdp36878

  A Cisco 7500 series router with Multiprotocol Label Switching (MPLS) configured might corrupt large packets that arrive on a channelized serial interface (CT1/CE1) and then switch to a tag MPLS-enabled interface. This situation occurs during the fragmentation process of the packet. Incoming tag MPLS packets are not affected.

  This situation only occurs for Route Switch Processor (RSP) switched packets. Versatile Interface Processor (VIP) distributed switching is not affected. There is no workaround.

- CSCdp42538

  A PA-A2 port adapter will not receive packets that are larger than 473 bytes. There is no workaround.

- CSCdp47338

  A Route Switch Processor (RSP) that is configured with Multiprotocol over ATM (MPOA) clients might reload. There is no workaround.

- CSCdp54245

  Multiprotocol over ATM (MPOA) shortcuts might not check for the frame sizes being sent on them. If the frame size exceeds the maximum transmission unit (MTU) size of the egress Multiprotocol over ATM Client (MPC), egress MPC drops the packet, resulting in the loss of connectivity.

  Workaround: Configure matching MTUs on either side of shortcuts (for example, all LAN Emulation Clients (LECs) that are served by ingress and egress MPCs should have the same MTU). If MTUs cannot be altered, then do not configure MPOA on both sides.

- CSCdp60101

  When configured to provide access control, the Kerberos client on Cisco products will fail all authentications when the expiration of the credential falls between January and February of a leap year.

  Workaround: Choose an alternate form of authentication such as Terminal Access Controller Access Control System Plus (TACACS+) or Remote Dial-In User Service (RADIUS).

Wide-Area Networking

- CSCdk39903

  After you enter the **show vpdn history failure** EXEC command, the console might lock up, and the CPU utilization might rise to 100 percent. This condition is most likely to occur if the history log has wrapped. There is no workaround.

- CSCdm59025

  After startup, a PPP interface might have an incorrect High-Level Data Link Control (HDLC) encapsulation string of 8F000800 instead of the correct FF030021 string.

  Workaround: Enter the **clear adjacency** EXEC command, or enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdm91461

  If you are using a Cisco 3640 router running Cisco IOS Release 12.0(5.3) and poll CISCO-CALL-HISTORY-MIB objects to track calls, you might see incorrect information returned for the object ciscoCallHistoryDestinationAddress. The same IP address repeats multiple times even though the corresponding ciscoCallHistoryDestinationHostName is always unique for the same instance. This bug has been fixed in Cisco IOS Release 12.0(08.00.02)T.

- CSCdp14536

  Under rare conditions, a Multiprotocol over ATM client/Multiprotocol over ATM server (MPC/MPS) will receive a route change from the Next Hop Resolution Protocol (NHRP) side of the cloud but will not purge the affected cache entry. There is no workaround.

- CSCdp18492

  A Cisco router might experience a software-forced reload because of watchdog timeout if thousands of switched virtual circuits (SVCs) or LAN Emulation (LANE) clients are configured on a single ATM interface.

  Workaround: Reduce the number of SVCs or LANE clients that are configured on the ATM interface.

- CSCdp21451

  A console buffer overrun might occur on a Cisco 1600 series router, a Cisco 3800 series router, a Cisco 800 series router, or a Motorola SMC (MPC860)-based platform if you initiate a PAD or X.28 outgoing connection from the console terminal. This problem does not occur if you make a PAD or X.28 connection from the vty lines.

  Workaround: Exit the console session, and then restart the console session.

- CSCdp25693

  The dialer idle-timeout might not reset for the inbound interesting packets on all serial interfaces except the first interface, which is configured with the **dialer idle-timeout either** interface configuration command for situations where fast switching is allowed. As a result, all interfaces except for the first serial interface drop the call.

  Workaround: Use process switching instead of fast switching so that all serial interfaces reset the idle timer as expected.

- CSCdp36081

  A Cisco 3640 router that is running Cisco IOS Release 12.0(7), might experience memory corruption and not be able to access core files. There is no workaround.

- CSCdp38620

  The Integrated Local Management Interface (ILMI) on a Cisco router might respond with the invalid value 0 instead of noSuchName when the interface is queried by the peer switch ILMI on ILMI MIB objects atmfAtmLayerIlmiVersion and atmfAtmLayerNniSigVersion. There is no workaround.

- CSCdp40742

  A Cisco router that is running Cisco IOS Release 2.0(7)S and supports a large number of ISDN Primary Rate Interfaces (PRI)s might reload due to low memory. There is no workaround.

- CSCdp50259

  If the Layer 2 link is lost while using X.25 over D-channel, a Cisco router will attempt to reestablish the link by using the terminal endpoint identifier (TEI) value of B-channel. The router will need to be reloaded to reestablish the X.25 connection. There is no workaround.

- CSCdp58434

  Enhanced Local Management Interface (ELMI) does not work correctly on a Cisco 3810 router that is running Cisco IOS Release 12.0(7)T. The router receives ELMI Status Enquiries, but does not acknowledge them. This situation does not occur in previous Cisco IOS releases. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(8)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(8). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdk92780

  A Cisco MC3810 series multiservice access concentrator that is connected by a serial interface to an AS400 Synchronous Data Link Control (SDLC) interface might experience problems keeping the line up. The line goes active on the AS400 side, and debugs in the router show one or two exchange identification (XID) frames from the host before the line goes down.

  Workaround: Configure idle character-marks in the interface of the router, and upgrade to Cisco IOS Release 12.0(7.1) or a later release.

- CSCdm40972

  When an X.25 interface initially comes up, IP route entries for its subinterfaces (if any) are not added to the IP routing table.

  Workaround: Restart X.25 to cause the subinterface routes to appear.

- CSCdm71463

  When "chassisType" is polled on a Cisco 7200 series router, the chassisType OID is returned as "Unknown." There is no workaround.

- CSCdp13010

  A Cisco router that is running Cisco IOS Release 11.1(28.1)CC and later releases with maximum transmission unit (MTU) configuration statements might see an unwanted cbus switching complex restart five minutes after booting. The switching complex restart only occurs if the MTU interface reconfiguration causes a MEMD recard because of a change in the MEMD buffer size used by the interface. There is no workaround.

- CSCdp17575

  If more than one channel or clock rate is larger than 64kbps, a Cisco MC3810 series multiservice access concentrator might not set the parity bit for the pointer field in the ATM adaptation layer 1 (AAL1) and generate bit errors. This situation occurs when the Cisco MC3810 series multiservice access concentrator is supporting T1 circuit emulation service (CES) and is connected to a device that is not a Cisco MC3810, but does not occur if both devices are Cisco MC3810 series multiservice access concentrators or if the circuit units are equal to or greater than six timeslots. There is no workaround.

- CSCdp23703

  A Cisco router might reload with a SegV error if you try to log in while the **debug callback** EXEC command is enabled.

  Workaround: Disable the **debug callback** EXEC command.

DECnet

- CSCdp00940

  If a Cisco router is running a Cisco IOS release earlier than Cisco IOS Release 11.3 and is using the DECnet Phase IV routing protocol, the DECnet network might experience routing loops for periods of time up to the value of the argument given in the **decnet routing-timer** *seconds* interface configuration command. These routing loops might start when a network link goes up or down, and DECnet traffic will be discarded while these loops occur.

  Workaround: Reduce the value given in the **decnet routing-timer** *seconds* interface configuration command.

- CSCdp25634

  If a Cisco router recognizes a Phase IV VAX cluster, the router will install a route to the cluster alias and advertise reachability to it across a Phase V attached network. It is possible for a routing loop to form if cluster aliases stop being advertised and if the two routers are connected in parallel between Phase IV and Phase V. If the router is the Phase IV designated router for the interface to which the VAX cluster is attached, there might be some connectivity issues between the VAX clients and the VAX cluster alias, but individual VAX machines can still be reached.

  Workaround: Set another router to be the Phase IV designated router for the LAN.

EXEC and Configuration Parser

- CSCdk64574

  A Cisco AS5800 access server might reload with a bus error after an ASCII login.

  Workaround: Upgrade to one of the following Cisco IOS releases: Cisco IOS Release 12.0(7) and later releases, Cisco IOS Release 12.0(7)T, Cisco IOS Release 11.3(10.6)AA, or Cisco IOS Release 12.0(7)S and later releases.

- CSCdp21558

  Performing NVGEN (that is, entering the **show running-config** command or entering the **write memory** command) might result in reloads for Cisco 2500, 2600, and 4000 series routers and spurious memory access in Cisco 3600 and 7200 series routers. You will not be able to see the running configuration. There is no workaround.

IBM Connectivity

- CSCdm71810

  Removing serial tunneling (STUN) statements from a serial interface and global interface causes a Cisco 7513 router to reload with a bus error.

  Workaround: Shut down the synchronous data link control (SDLC) interface before removing the STUN statement.

- CSCdm89688

  A Cisco 7000 series router with two CIP cards that are both running the **tn3270-server** interface configuration command might unexpectedly reload with a software forced crash if you remove the **client ip** configuration command. There is no workaround.

- CSCdm89739

  If you are configuring a Cisco 2600 series router by entering the **fras ban** interface configuration command with the **fras ddr-backup** interface configuration command, the backup is driven if the primary interface goes down. When the backup interface goes down, the backup enabled by the **fras ddr-backup** interface configuration command switches to the main interface. But if the backup interface goes down and the main interface goes up, the sessions are not recovering, and **fras ddr-backup** tries the backup interface even though the backup interface is in a down state.

  Workaround: Disable **fras ddr-backup** on the main interface by entering the **no fras ddr-backup** interface configuration command.

- CSCdm91465

  A Cisco 2500 router might exhibit the following error message on a Binary Synchronous Communications Protocol (bisync) interface:

  ```
  LINK-2-INTVULN
  ```

  There is no workaround.

- CSCdp03857

  A Cisco 4000 router or a Cisco 2500 router that is running Cisco IOS Release 12.0(6.5) and data-link switching (DLSw) will not be compatible with other platforms. This condition does not affect other platforms that are running DLSw. There is no workaround.

- CSCdp04887

  An Advanced Peer-to-Peer Networking/Dependent LU Requester (APPN/DLUR) router might reload with the following stacktrace:

  ```
  RA: 0x60703538[h(0x6070345c)+0xdc]
  RA: 0x607038E0[fsm_receive_router(0x607035b0)+0x330]
  RA: 0x606E285C[upchuck(0x606e2654)+0x208]
  RA: 0x606E2348[rcv_cls_msg(0x606e2080)+0x2c8]
  RA: 0x606E1ED8[dlcdx_process_messages(0x606e1eb8)+0x20]
  RA: 0x607027D0[xxxpcasm(0x60702440)+0x390]
  ```

  There is no workaround.

- CSCdp09801

  An Advanced Peer-to-Peer Networking (APPN) router might reload in cs_process_lsa_ips during a link activation and deactivation timing window. There is no workaround.

- CSCdp14927

  If both a primary Dependent LU Server (DLUS) and a backup DLUS are configured on an Advanced Peer-to-Peer Networking/Dependent LU Requester (APPN/DLUR) router, the router might unnecessarily time out an allocate to one DLUS after having to time out an allocate to the other DLUS. When this situation occurs, you will receive an “allocate has an invalid rcb 0. Restart TP.” message.

  Workaround: Enter the **prefer-active-dlus** configuration command with the “no retries” operand. If you have prefer-active-dlus coded on the APPN control point with no retries, only the currently active DLUS will be retried. This is a temporary workaround.

- CSCdp17578

  An Advanced Peer-to-Peer Networking (APPN) router might experience a memory leak if you save the Routing Information Field during link activation. There is no workaround.

- CSCdp24638

  If you are running source-route bridging (SRB) over Frame Relay (RFC 1490), the following traceback appears on the console:

  ```
  %LINK-3-BADMACREG: Interface Serial1.50, non-existent MACADDR registry for link 43
  -Process= “LanNetMgr Supt”, ipl= 0, pid= 76
  -Traceback= 6080DA8C 6080D8FC 60DEBE1C 60DE04B8 60DFA820 60DFAA60 6031A984 6031A970
  ```

  There is no apparent impact.

  Workaround: Enter the **lnm disabled** global configuration command.

Interfaces and Bridging

- CSCdk74973

  When used with a channelized serial interface (CT1/CE1), compression service might be interrupted if there is any system-wide service interruption like online insertion and removal (OIR) or micro reload. There is no workaround.

- CSCdm35733

  FEBE line and path counters on a POS interface might not increment with the following images: rsp-jv-mz.111-18.CC.bin, rsp-jv-mz.111-24.CC.bin, and rsp-jsv-mz.120-3.0.2. There is no workaround.

- CSCdm47892

  A Cisco 7500 series router that is running the rsp-jsv40-mz (Enterprise 40) software image on Cisco IOS Release 11.3(9.2)T might experience a bus error. A stack trace decode reveals the following:

```
0x40262B9C:__start(0x60010000)+0xe0252b9c
0x60093B08:tr_bcast(0x60093af8)+0x10
0x60250630:rsp_tx_start(0x60250258)+0x3d8
0x601DA4D4:datagram_out(0x601d9d5c)+0x778
0x6070FC70:llc_wput(0x6070ec6c)+0x1004
0x60925134:CLSSapUDataStnReq(0x60924fec)+0x148
0x60921858:CLSSapHandleMsg(0x60921710)+0x148
0x6091EA10:CLSDluSendToSap(0x6091e948)+0xc8
0x60925B38:CLSWritePut(0x60925a74)+0xc4
```

  There is no workaround.

- CSCdm60927

  A Bridge-Group Virtual Interface (BVI) might become wedged intermittently (approximately monthly).

  Workaround: Create a new BVI.

- CSCdm77025

  Running Link Access Procedure, Balanced (LAPB) under a heavy traffic load might cause frames to get lost within the router, which results in REJECTS, backup of output queue, and output drops. There is no workaround.

- CSCdm79792

  A Cisco router might reload immediately after you enable STAC compression. This condition occurs with High-Level Data Link Control (HDLC) encapsulation when FastPath packets or particles are present in the output queues when compression is enabled.

  Workaround: Enter the **no ip route-cache** interface configuration command before enabling compression, or perform a shutdown on the line before enabling compression.

- CSCdp11141

  A Cisco router that is running Cisco IOS Release 12.0 might not reply to an Address Resolution Protocol (ARP) request if the Ethernet port is set for bridging and is in blocking mode. There is no workaround.

- CSCdp12182

  Integrated Local Management Interface (ILMI) might not come up if you are using a PA-A3 port adapter and running Cisco IOS Release 12.0(6.5) or later. There is no workaround.

- CSCdp23738

  Uneven numbered interfaces (that is, SerX/1 and SerX/3) on a PA-4E1 (75/120) four-port serial card might not work properly on Cisco 7200 series and Route/Switch Processor (RSP) routers. The following Cisco IOS releases are affected, including later release versions: Cisco IOS Release 12.0(6.5); Cisco IOS Release 12.0(6.5)T; Cisco IOS Release 12.0(6.5)S; Cisco IOS Release 12.0(6.5)PI01; Cisco IOS Release 11.1(29)CC, and Cisco IOS Release 12.0(6.6)SC01.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdm82319

  If you run an H323 application, such as NetMeeting, the deletion of Network Address Translation (NAT) entries created for H323 will not free the allocated buffer completely and will cause a memory leak. The NAT entry data structure that tracks H225 and H245 information is not being freed when the NAT entry is deleted. There is no workaround.

- CSCdp04554

  Enhanced Interior Gateway Routing Protocol (EIGRP) might derive the metric of a summary from a route outside the summary that has the same prefix and shorter masks. There is no workaround.

- CSCdp05306

  After a link flap, the summary route might not appear in the routing table even though it appears in the OSPF topology table.

  Workaround: Restart the OSPF process, or reload the router.

- CSCdp05327

  The following entries might be added to the running configuration of a Cisco router even though Network Address Translation (NAT) is not configured:

  ```
  ip nat translation timeout never
  ip nat translation tcp-timeout never
  ip nat translation udp-timeout never
  ip nat translation finrst-timeout never
  ip nat translation syn-timeout never
  ip nat translation dns-timeout never
  ip nat translation icmp-timeout never
  ```

  There is no workaround.

- CSCdp15166

  When fast policy switching is enabled on dialer interface on a Cisco router that is running Cisco IOS Release 11.3(9)T or 12.0(7) a packet is not fast switched, and process switching is used instead. There is no workaround.

- CSCdp27183

  A Resource Reservation Protocol (RSVP) message will be dropped if the flags or reserved fields in the common header are not set to zero. In this situation, you will not be able to operate within implementations that use these fields for new features. There is no workaround.

ISO CLNS

- CSCdm48924

  While displaying the output of the **show isis topology** command, a Cisco router might reload. There is no workaround.

- CSCdp12169

  Cisco IOS Release 12.0(6.2)T might break Point-to-Point Protocol (PPP) over ATM on a Cisco 4500 router with AAL5SNAP encapsulation enabled. There is no workaround.

Miscellaneous

- CSCdj88748

  The individual timeslots in a fractional T1/E1 circuit emulation service (CES) circuit might get misaligned if an ATM uplink switchover or reroute occurs, and the content in each timeslot remains error free even though the whole fractional circuit cannot be synchronized. This situation occurs on Cisco 7200 series routers with PA-A2 port adapters with (CES) and Cisco LightStream 1010 5 Gbps modular switches with (CES) and pulse amplitude modulation (PAM).

- CSCdk56600

  The Ascend-Idle-Limit attribute is defined as being a value in seconds, and when this attribute is applied to a client using PPP mode, the value is retained in seconds. But if the Ascend-Idle-Limit attribute is applied to a client that is using PPP interactive mode, the attribute is converted into a value of minutes. For example, both 1 second and 59 seconds are treated as 1 minute. There is no workaround.

- CSCdk61320

  When you perform an encrypted Kerberized Telnet to a Cisco 7500 series router, the initial setup goes fine, but nonsense output results when the decryption of packets from the router occurs on the client side. There is no workaround.

- CSCdm06470

  A Cisco router might reload if you enable Hot Standby Router Protocol (HSRP) on a cable interface because HSRP does not function properly on cable interfaces. There is no workaround.

- CSCdm15911

  If you are using IP Security (IPsec) in transport mode over a dialer with Multilink PPP and PPP compression, a Cisco router might exhibit the following error message:

  ```
  %SYS-2-GETBUF: Bad getbuffer, bytes= 58332 -Process= “Encrypt Proc”, ipl= 0, pid= 43
  ```

  and traceback:

  ```
  IPSEC(encapsulate): locally-sourced pkt w/DF bit set is too big, ip->tl=62324, mtu=1432
  ```

  Workaround: Configure tunnel mode IPSec, or disable PPP compression.

- CSCdm33707

  After a Cisco router is reloaded, the Encryption Service Adapter (ESA) cannot reestablish an active crypto connection.

  Workaround: Remove the crypto map, reload the router, and reapply the crypto map.

- CSCdm33977

  In circumstances of increased stress and constant changes, a Cisco router that has a large number of adjacencies on a multiaccess network and is using distributed Cisco Express Forwarding (CEF) might display some prefixes in the LC that are not in the main Route Processor (RP) table. There is no workaround.

- CSCdm62412

  Spatial reuse protocol (SRP) hardware might receive and drop giant packets under OC-12 line rate traffic with the Versatile Interface Processor (VIP) stressing memory usage. This condition might occur in a tag switching configuration over paths that require the fragmentation of tag-encapsulated IP packets. There is no workaround.

- CSCdm86777

  A Cisco 7200 series router might not switch packets when crypto map is configured. This situation occurs when you enable Cisco Express Forwarding (CEF) switching. Symptoms might include a connection activity display of twice the normal number of encrypted and decrypted packets than for the peer router when you enter the **show crypto cisco connections** privileged EXEC command. There is no workaround.

- CSCdm94728

  Traffic to a Versatile Interface Processor (VIP) might not be routed properly on a Cisco 7500 or 7200 series router that is running Cisco IOS Release 10.3(6.3) if the destination link is encrypted using Cisco Encryption Technology (CET). There is no workaround.

- CSCdp00331

  IP Security (IPSec) might not function properly if you are running Cisco IOS Release 12.0(6.3)T. There is no workaround.

- CSCdp05176

  Priority queueing might not function properly with a protocol type-code access list on Cisco 2600 series routers. There is no workaround.

- CSCdp05948

  Attributes 197 and 255 in the RADIUS accounting stop record are recorded as “0” on a Cisco 2600 series routers and Cisco 3600 series routers that are running Cisco IOS Release 12.0(5)T1. There is no workaround.

- CSCdp07039

  Cisco 1700 series routers and Cisco 2600 series routers that are running Cisco IOS Release 12.05 T cannot start ISAKMPA SA using the rsa-encr authentication method. The debug output reports that “Hash payload is incorrect!” There is no workaround.

- CSCdp07404

  You might receive LINK-2-INVTULN traceback messages on Asynchronous Security Protocol (ASP) interfaces. This situation can occur on any Cisco router. There is no workaround.

- CSCdp07476

  When you enable bridging on a Fast EtherChannel (FEC), the host functionality might not work properly, but bridging functionality is not affected. There is no workaround.

- CSCdp13469

  Distributed Cisco Express Forwarding (dCEF) might not function properly on PA-T3 High-Speed Serial Interfaces (HSSI) port adapters, and traffic on the interface is not switched by distributed switching after a large number of interface reset events occur. There is no workaround.

- CSCdp16515

  A Cisco router will reload if IP Security (IPSec) is enabled with fast switching on links that use PPP encapsulation with PPP compression. There is no workaround.

- CSCdp21248

  If distributed Cisco Express Forwarding (dCEF) and Cisco Encryption Technology (CET) are enabled on a Versatile Interface Processor (VIP), encrypted traffic from the VIP to a non-VIP interface will be process switched. There is no workaround.

- CSCdp21739

  Changing the status of the interface on a PA-A3 port adapter might cause routes to be removed from the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table.

  Workaround: Issue the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdp23921

  Under rare conditions, a Cisco RSP7000 router that is running Cisco IOS Release 12.0(6.6) with a Versatile Interface Processor (VIP) interface might refuse to send or receive any encrypted traffic. Once the interface gets into this state, it will drop all encrypted traffic until either you reload the router, or disable encryption and reenter the crypto map.

  To determine whether a VIP is in this condition, you can enter the **show crypto map** EXEC command and the **show crypto cisco connections** privileged EXEC command. If the crypto map is listed with a negative connection ID that does not appear in the crypto connection table, then this problem is occurring.

  There is no workaround.

- CSCdp24644

  If devices that can share the same IP address at different times are connected behind an MPC, some Multiprotocol over ATM (MPOA) shortcuts might not be valid after they switch over the IP address. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdk67783

  IPX allows the primary interface and multiple ISL subinterfaces to have the same IPX network number and encapsulation.

  Workaround: Do not configure interfaces with the same IPX network number.

- CSCdp13795

  If you are using IPX Enhanced Interior Gateway Routing Protocol (EIGRP), you might experience an inconsistency in Service Advertising Protocol (SAP) updates on a remote router if the serial interface is brought down for a brief time and then brought up.

  Workaround: Enter the **clear ip eigrp neighbors** EXEC command or enter the **no ipx linkup-request sap** interface configuration command for the serial interfaces.

- CSCdp19523

  If an IPX route goes down in a multiple path topology, the 85XX lower layer switch engine might get out of synchronization with the Layer Three IPX routing table. A lower layer forwarding and switching anomaly might occur if the router first receives a “down” notification for a network from the same host that originally notified the router about that network and then the router shortly afterwards receives a good route to the network from another host. There is no workaround.

Wide-Area Networking

- CSCdk07546

  Retransmitted frames by an Advanced Peer-to-Peer Networking (APPN) router using remote source-route bridging are truncated. There is no workaround.

- CSCdk43155

  After upgrading to Cisco IOS Release 11.3, you might occasionally experience the following error message:

  ```
  %X25-3-X25INT: Interface ?, X.25 internal error Invalid lock operation on an X.25 route
  -Process= “X.25 Background”, ipl= 2, pid= 69
  ```

  Workaround: Remove the route entry associated with the destination from the X.25 routing table, and then add it back again.

- CSCdm02785

  Entering the **x25 map cmns** global configuration command causes a Cisco 2600 series router running Cisco IOS Release 11.3 to reload with a SegV exception.

  Workaround: Use the equivalent **x25 route** global configuration command.

- CSCdp36081

  A Cisco 3640 router that is running Cisco IOS Release 12.0(7), might experience memory corruption and not be able to access core files. There is no workaround.

- CSCdm37706

  When standby time arrives on a BRI that is used for backup of a serial interface, a disconnect on q931 is never sent. The ISDN switch needs to declare remote terminal equipment out of order. There is no workaround.

- CSCdm45948

  An RSP4 and a Cisco 7500 series router that are running Cisco IOS Release 12.0(4a) might reload at “set_if_input.”

  Workaround: Disable Cisco Express Forwarding (CEF).

- CSCdm46165

  A Cisco router might display a “%TCP-2-INVALIDTCPENCAPS” message, but the system does not lock. There is no workaround.

- CSCdm66787

  The Link Access Procedure, Balanced (LAPB) module will retransmit any outstanding unacknowledged frames when the remote device reports “Receiver Ready” after previously reporting “Receiver Not Ready.” If the T1 timer has not expired while the remote device was not ready, the outstanding unacknowledged frames should still be considered outstanding, and the LAPB should not retransmit them. There is no workaround.

- CSCdm67523

  A Cisco 7507 router with an ATM Interface Processor (AIP) installed might reload with the following error and not come back up unless the AIP is removed:

  ```
  %DBUS-3-CXBUSERR: Slot 1, CBus Error
  %RSP-3-ERROR: CyBus0 error 10
  %RSP-3-ERROR: command/address mismatch
  %RSP-3-ERROR: bus command write 4bytes (0xE)
  %RSP-3-ERROR: address offset (bits 3:1) 4
  %RSP-3-ERROR: virtual address (bits 23:17) 000000
  ```

  There is no workaround.

- CSCdm79305

  A Protocol Translation that is configured with Virtual Async and is running over an X.25 connection might not transmit a full packet when the X.25 output maximum packet size is set to 512 bytes and above. There is no workaround.

- CSCdm80044

  A Cisco router might reload with a bus error in xot_cx_transition. The stack decodes might vary. There is no workaround.

- CSCdm93360

  A Cisco router that is performing X.25 permanent virtual connection (PVC) switching might experience the following error message if a resend is received on the incoming PVC while the outgoing PVC is not active:

  ```
  %X25-3-X25INT: Interface ?, X.25 internal error unable to walk VC output queue
  ```

  There is no workaround.

- CSCdp00520

  The backup interface function does not work if the backup interface is on a 2A/S WAN interface card network module and is configured with the **physical-layer async** interface configuration command. If the primary interface fails, the backup interface will attempt to dial, but it will be unsuccessful.

  Workaround: Use a different network module for the backup interface if you are configuring it using the **physical-layer async** interface configuration command. If you are using the 2A/S network module, and the 2A/S network module is in a lower slot number than the primary interface, the backup functionality will work.

- CSCdp01840

  Excessive CPU utilization might be given to the dialer software component while making multiple digital calls to an ISDN PRI router. These CPU HOGS will cause a Route Switch Processor with 10 busy PRIs to become unusable. There is no workaround.

- CSCdp02738

  Multilink fragments that are sent over an X.25 link might not have an High-Level Data Link Control (HDLC) header around the PPP packet. This situation can cause the receiving side to be off by 2 bytes when it searches for the protocol of a packet. If the **debug ppp** {**negotiation**} EXEC command has been enabled, you might receive an error message similar to the following:

  ```
  Vi1 UNKNOWN(0x4000): Non-NCP packet, discarding
  ```

  There is no workaround.

- CSCdp03096

  If a Cisco router with a Versatile Interface Processor (VIP) is running Cisco IOS Release 12.0(6.3), the VIP might run at 99 percent CPU utilization. This situation occurs when packets are received on a VIP and should be routed to an interface where the tx-queue-limit is set to a low value like 3. The VIP will buffer the packets and fail to transfer them to the outbound interface.

  Workaround: Configure the tx-queue-limit to a higher value on the outbound interface.

- CSCdp05956

  A Cisco 3640 router that is running Cisco IOS Release 12.06(6.3) might reload after running for a few minutes. There is no workaround.

- CSCdp13681

  A Cisco AS5300 universal access server that is running Cisco IOS Release 12.0(6.3)T might reload with a bus error. There is no workaround.

- CSCdp21451

  A console buffer overrun might occur on a Cisco 1600 series router, a Cisco 3800 series router, a Cisco 800 series router, or a Motorola SMC (MPC860)-based platform if you initiate a PAD or X.28 outgoing connection from the console terminal. This problem does not occur if you make a PAD or X.28 connection from the vty lines.

  Workaround: Exit the console session, and then restart the console session.

Resolved Caveats—Cisco IOS Release 12.0(7)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(7). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdm43418

  Traffic shaping with FRF9 compression might not work properly on a Cisco 3640 router with a compression service adapter (CSA). There is no workaround.

- CSCdm52927

  A Cisco router might reload under rare, timing-related circumstances if you attempt to delete rows in the ciscoPingTable of the CISCO-PING-MIB. There is no workaround.

- CSCdm78286

  A Cisco 7500 series router that is running Cisco IOS Release 12.0(5) might experience high CPU utilization when using a VIP-2 service adapter with hardware encryption. There is no workaround.

- CSCdm79977

  When an interface processor is experiencing a hardware or software problem, it is possible for the Route Switch Processor (RSP) CPU to experience nearly complete utilization while it performs switching-complex restarts in a attempt to recover the failed card. There is no workaround.

- CSCdm82691

  A Cisco router running Cisco IOS Release 12.0(6) Route Switch Processor (RSP) code with a Versatile Interface Processor (VIP)-based, channelized E1, T1, 4T, or 8T port adapter might exhibit the following error message:

  ```
  %RSP-3-BADBUFHDR: Invalid buffer ptr, address 58000000
  -Traceback= 6025DD38 60266EB8 60237798 00:33:29:
  %RSP-3-INVRTN: Invalid return queue, next=0x61323238, hwidb=0x617A0A80, type=0x0
  queue_ptr=0x130, bufhdr_offset=0x0, id=0, bcast_id=0 bufhdr 58007420: 00000000 00000128
  01280000 00000000
  -Traceback= 60266E74 6023779800
  ```

  There is no workaround.

IBM Connectivity

- CSCdm37638

  A Cisco 4500 or 4700 series router with an NP-2R Token Ring might pause indefinitely approximately once a week and display the following error message:

  ```
  %SYS-2-INPUTQ: INPUTQ set, but no IDB
  ```

  This condition is not effected by the revision level of the motherboard. There is no workaround.

- CSCdm51285

  A Cisco router might reload with a Segv exception error with the following stack trace:

  ```
  System was restarted by error - a SegV exception, PC
  0x8084D788[k_convSdllcPortEntry_get(0x8084d67c)+0x10c] k_convSdllcPortEntry_get
  convSdllcPortEntry_get GetNextObjectInstance do_response do_snmpv1 do_mgmt snmp_engine
  ip_snmp
  ```

  Workaround: Delete the entry in the ASN.1 private Cisco MIB that is causing the router to reload.

- CSCdm55118

  A Cisco router using Advanced Peer-to-Peer Networking (APPN) may consume excessive CPU resources while issuing messages during a locate storm. The “XXXTPD02_LOGMSG_01” message might appear repeatedly. There is no workaround.

- CSCdm59024

  A data-link connection might not recover when the Advanced Peer-to-Peer Networking (APPN) link is not restarted, although the router is configured to retry repeatedly. This situation occurs when a Cisco 4700 router is defined as an APPN network node with an APPN link across Frame Relay RFC 1490 to an IBN NN950 that is configured as a network node. There is no workaround.

- CSCdm64065

  No SNA traffic passes between a server and a Cisco Network Node router when the network node uses DLSw flow control to disallow the sending of further SNA traffic by the server. There is no workaround.

- CSCdm67191

  A Dependent logical unit Requester physical unit (DLUR-PU) might appear stuck in a “stopping” state while waiting for a deactivate physical unit (DACTPU) request from a Dependent logical unit server (DLUS). In this situation, the DLUS has already cleaned up this PU, and the PU is in a connectable state on virtual telecommunications access method (VTAM). The DLUR cannot clean up this PU until it receives the DACTPU request. This software change allows DLUR-PUs that have waited for this DACTPU for more than 2 minutes to issue another REQDACTPU request to the DLUS. If the DLUS has already cleaned this PU, it will respond negatively to the REQDACTPU. This negative response will initiate the cleanup of this PU by the DLUR. There is no workaround.

- CSCdm71190

  An Advanced Peer-to-Peer Networking (APPN) network node router might not allocate the conwinner session of its dual control point-to-control point session with an adjacent end node. The conloser session is set up correctly, but the conwinner session fails in sense 0x80140003 if you issue the **debug appn ss** command.

  Workaround: This situation results if you change an adjacent network node to an end node. Cycle the link for the end node that you changed.

- CSCdm72581

  After continuously looping in nns_olu_cdinit_reply_processing, an Advanced Peer-to-Peer Networking (APPN) router running Cisco IOS Release 11.2 might reload and exhibit the following error message:

  ```
  abort crashdump process_handle_watchdog signal_receive process_forced_here
  nns_olu_cdinit_reply_processing
  ```

  There is no workaround.

- CSCdm73345

  A Cisco router running Advanced Peer-to-Peer Networking (APPN) might not respond to BINDs or fail BINDs in sense 0x08150004. There is no workaround.

Interfaces and Bridging

- CSCdk60571

  Serial interfaces and line protocols on Cisco 3600, 7200, and 7500 series routers might fail with all physical control signals up, including data carrier detect (DCD).

  Workaround: Perform a microcode reload.

- CSCdk66951

  When you are configuring a new E1 PRI interface on a port adapter in a VIP2-based system, all active E1 interfaces will fail even if those E1 interfaces are not on the same VIP2. There is no workaround.

- CSCdk89313

  In certain Cisco IOS releases there is currently no NetFlow support for Bridge-Group Virtual Interfaces (BVIs) or any other interfaces in a bridge group. The resolution is to upgrade to a Cisco IOS release that support this feature. There is no workaround.

- CSCdm28550

  If the ATM interface on a Cisco 7000 series router receives an ATM adaption Layer 5 (ATM5) packet of 66532 bytes, it might result in an internal zero length packet and cause the Versatile Interface Processor (VIP) to reload. There is no workaround.

- CSCdm45222

  An ATM interface on a Cisco router might drop Operation, Administration, and Maintenance (OAM) packets and exhibit increasing ignores and drops with distributed Cisco Express Forwarding (dCEF) and an input feature (such as Access Control List) configured. There is no workaround.

- CSCdm61507

  If you enter the **show frame-relay pvc** command on a Cisco router with FRF9 compression enabled, the incoming packet count might be doubled, first in its compressed state and then in its uncompressed state.

  Workaround: Disable FRF9 compression.

- CSCdm69501

  A Versatile Interface Processor (VIP) might reload with distributed Cisco Express Forwarding (dCEF) switching locally between subinterfaces with different maximum transmission unit (MTU) size on a PA-A1 port adapter.

  Workaround: Do not use distributed switching.

IP Routing Protocols

- CSCdk52593

  An external SPF calculation might be triggered every 35 to 40 seconds if there is an OSPF external link-state advertisement (LSA) containing a forwarding address that OSPF has no route for and if there is a static route to this forwarding address pointing to an OSPF enabled interface.

  Workaround: Remove the static route, or prevent the unreachable forwarding address from being included in the external LSA. To avoid the unreachable forwarding address, make sure that any autonomous system boundary routers (ASBRs) redistributing between different OSPF domains have the fix for CSCdi63983.

- CSCdm51483

  Entering the **show ip igmp group** command might cause a bus error reload if an IGMP entry is deleted during the command execution. This condition occurs intermittently. There is no workaround.

- CSCdm67167

  A Cisco 8540 Multiservice Switch Router might reload if you use a prefix list with range entries when entering the **route-map** command for default origination.

  Workaround: Use an access-list rather than a prefix list when entering the **route-map** command for default origination, or avoid using range entries in a prefix list.

- CSCdm70876

  A router with IP Protocol Independent Multicast (PIM) enabled might reload when you enter the **no ip sdr** command. This condition occurs under the following conditions:

  – The subject router is the Internet Group Management Protocol (IGMP) querier.

  – There are a large number of external IGMP reporters.

  – Session Directory Protocol (SDR) is the last group locally joined at the subject router's subject interface.

  – You enter the **no ip sdr** command shortly after entering the **no ip pim** command.

  There is no workaround.

ISO CLNS

- CSCdm46511

  A Cisco router using Connectionless Network Service (CLNS) over X.25 encapsulation might reload and exhibit the following error message:

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
-Traceback= ........ ........ ........ ........ ........ ........ ........
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= ........ ........ ........ ........ ........ ........ ........
%SYS-2-MALLOCFAIL: Memory allocation of 48 bytes failed from 0x........, pool Processor,
alignment 0 -Process= “{interrupt level}”, ipl=3
-Traceback= ........ ........ ........ ........ ........ ........ ........
```

  Workaround: Turn off the generation of CLNS error protocol data units (PDUs) on all interfaces by entering the **no clns send-erpdu** command. In addition, you should investigate and resolve any X.25 encapsulation problems.

LAT

- CSCdm82005

  The following line commands are not supported in Cisco IOS Release 12.0(5.5) through 12.0(6): the **session-limit** command, the **absolute-timeout** command, and online help for the **lat** command. There is no workaround.

Miscellaneous

- CSCdk41197

  A Multiport Basic Rate Interface (MBRI) might pause indefinitely in "awaiting establishment" and "tei assigned" modes. Entering the **clear interface bri** *interface number* command establishes multiple frames on the port and allows another ISDN call to be made. There is no workaround.

- CSCdk58186

  Half duplex should only be configured on an interface that is configured with a half duplex protocol (such as SDLC) or bisynchronous encapsulations.

  Workaround: Configure the interface for full duplex when not specifically running a half-duplex protocol. The interface command to do this is **full-duplex**.

- CSCdm00627

  A Cisco AS5800 router shelf might reload because of a bus error after configuring "ds0 busyout" when calls are up on the controller. There is no workaround.

- CSCdm04888

  If you change the media type for an Ethernet interface from auto select to 10BaseT, the default configuration might change to AUI. An explicit interface reset will bring up the interface correctly.

  Workaround: Set media-type to auto-select.

- CSCdm13853

  A Cisco 3600 series router connecting via serial interface using WIC-1T to an AS/400 Synchronous Data Link Control (SDLC) interface might experience problems keeping the line up. After the line goes active on the AS/400 side, debugs in the router show one or two exchange identification (XID) frames from the host right before the line goes down. There is no workaround.

- CSCdp22947

  In Cisco IOS Release 12.0(7.1) and Cisco IOS Release 12.0(7.2), Address Resolution Protocol (ARP) replies are not sent for static Network Address Translation (NAT) entries. For example, the router does not respond to ARP requests for 2.2.2.3 from the **ip nat inside source static** *1.1.1.1 2.2.2.3* static NAT command.

  Workaround: Upgrade to a later release.

- CSCdm25998

  Traffic shaping is not working on a Fast Ethernet Interface on a Cisco 4700 router with Fast Switching enabled. There is no workaround.

- CSCdm47012

  Smart Modular and Sharp Flash cards using the LH28F016SCT chip set might report unrecoverable write errors on several Cisco platforms, including 7200 series, 7500 series, and GSR routers. The original Smart Modular and Intel Flash Cards are not affected. There is no workaround.

- CSCdm48366

  When entering the **crypto-map** *map-name* command on a Versatile Interface Processor (VIP) interface, you must use a name that is not a subset of another crypto map's name. For example, the interface recognizes "testtag1," "testtag10," and "testtag100" as the same crypto map names. There is no workaround.

- CSCdm51060

  When software compression is configured on a Cisco 7200 series router on an interface configured for Cisco Express Forwarding (CEF) or NetFlow switching, the router might experience a bus error failure and reload. This situation occurs because CEF and NetFlow switching are not disabled when compression is configured even though compression is not supported in CEF, NetFlow, or any fast-switching mode on a Cisco 7200 series router.

  Workaround: Explicitly disable CEF or Flow switching on the interface configured for compression by entering the **no ip route-cache** {**cef** | **flow**} command.

- CSCdm59007

  The Systems Network Architecture (SNA) packets might not be forwarded over a 64k leased line with High-Level Data Link Control (HDLC) encapsulation. There is no workaround.

- CSCdm63884

  A Cisco router might systematically reload with an error message if "num-exp 1* *" is configured on the router. There is no workaround.

- CSCdm68773

  A Cisco router might reload when the Cisco Service Manager (CSM) tries to allocate modems from a different pool. There is no workaround.

- CSCdm68811

  Hot Standby Router Protocol (HSRP) does not work if Inter-Switch Link (ISL) encapsulation is configured. The active router does not respond to an Internet Control Message Protocol (ICMP) ping of the virtual IP address.

  Workaround: Load a new image that contains a fix for this problem.

- CSCdm68862

  Hot Standby Router Protocol (HSRP) does not work when IP Protocol Independent Multicast (PIM) is configured on a Fast Ethernet interface that uses the DEC211140 chipset. The active router does not reply to an Internet Control Message Protocol (ICMP) ping of the virtual IP address.

  Workaround: Use the burned-in address by entering the **standby use-bia** command.

- CSCdm69227

  A Cisco 2600 series router that is running Cisco IOS Release 11.1(27)CC, 11.1(27.01)CC, 11.002(019.001), 11.2(19.01)P, 12.0(05.04)PI06, 12.0(05.05)S, 12.0(05.05)T, 11.2(19.01)BC, 11.1(27)CT, 12.0(05.05)SC, or 11.1(27.01)CT might exhibit the following rate-limited error message:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=1, ...
  ```

  The router should continue to function normally. There is no workaround.

- CSCdm70085

  A Cisco router running Cisco IOS Release 12.0(5.4) encryption image might reload if you enter the **crypto cisco pregen-dh-pairs** command. There is no workaround.

- CSCdm72498

  V.120 connections on a Cisco AS5800 access server might fail if you enter the **vty-async virtual-template** command and 144 or more virtual-access interfaces are in use and a new one is needed. On a failing connection, a “debug vtemplate” might show the following error messages:

  ```
  Vi202 VTEMPLATE: Messages from (un)cloning ... interface Virtual-Access1/0/58
  Vi202 VTEMPLATE: Messages from (un)cloning ... default ip address
  Vi202 VTEMPLATE: Messages from (un)cloning ... % Incomplete command
  ```

  Workaround: Keep the number of virtual-access interfaces under 144.

- CSCdm74852

  On a Cisco 3600 series router running Cisco IOS Release 12.0, IP MAC accounting only works with process-switched packets. There is no workaround.

- CSCdm79007

  Cisco Express Forwarding (CEF) fails between Token Ring Inter-Switch Link (TRISL) and either Ether-ISL or Ethernet.

  Workaround: Disable CEF switching and run standard fast switching.

- CSCdm80843

  You should not attempt to remove a PCMCIA card while accessing it. There is no workaround.

- CSCdm84669

  A Cisco 7200 or 7500 series router that is running Cisco IOS Release 12.0 and using encrypted connections like Cisco Encryption Technology (CET) or IP Security (IPSec) over High-Speed Serial Interface (HSSI) serial boards might fail. After the failure, no encrypted traffic can be sent over the connection until the router reloads, but unencrypted traffic is not affected. There is no workaround.

- CSCdm84682

  If you shut down a PA-A2 circuit emulation service (CES) circuit, you will bring down OAM-managed data PVCs that are defined on the same card. There is no workaround.

- CSCdm84931

  A Cisco router that is running Cisco IOS Release 12.0(6.1) will fail to authenticate an Entrust CA server. Entrust CA cannot be used with Cisco IOS Release 12.0(6.1). There is no workaround.

- CSCdm86777

  A Cisco 7200 series router might not switch packets when crypto map is configured. This situation occurs when you enable Cisco Express Forwarding (CEF) switching. Symptoms might include a connection activity display of twice the normal number of encrypted and decrypted packets than for the peer router when you enter the **show crypto cisco connections** command. There is no workaround.

- CSCdm94728

  Traffic to a Versatile Interface Processor (VIP) might not be routed properly on a Cisco 7500 or 7200 series router that is running Cisco IOS Release 10.3(6.3) if the destination link is encrypted using Cisco Encryption Technology (CET). There is no workaround.

Protocol Translation

- CSCdm69108

  TCP to X.25 permanent virtual circuit (PVC) translation might fail and cause the connection to be lost. There is no workaround.

Wide-Area Networking

- CSCdj39383

  A Cisco router with over 180 data-link connection identifiers (DLCIs) cannot boot properly because of excessive console log messages related to the startup of Frame Relay PVCs. There is no workaround.

- CSCdm28510

  Adding the **dialer isdn short-hold** command to the **map-class dialer** command to optimize ISDN costs based on AOC-D messages might break the "dialer idle-timeout" configuration. The idle timer resets to 4294966 seconds when expiring, and does not disconnect the ISDN call. The short-hold timer gets incremented on receipt of an AOC-D message, and never disconnects the ISDN call.

  Workaround: Remove the **dialer isdn short-hold** command from the **map-class dialer** command.

- CSCdm41493

  A Cisco 2600 series router that is running Cisco IOS Release 11.3(9)T might reload during an X.25-to-TCP translation.

  Workaround: Disable the "pt-vty-logging" service by issuing the **no service pt-vty-logging** command.

- CSCdm46082

  Multilink PPP does not work if Context-Based Access Control (CBAC) and Network Address Translation (NAT) configured on a Cisco 3600 series router.

  Workaround: Turn off Multilink PPP.

- CSCdm46683

  A Versatile Interface Processor (VIP) card might not respond to a RSP board's request for a DBUS transaction. The RSP will reset the VIP interface and perform a CBUS complex restart to reallocate MEMD.

  Workaround: Get in and out of the if-console for all the VIPs in the box.

- CSCdm49685

  After you reload a Cisco router, the ATM interfaces might assume the default User-Network Interface (UNI) value (3.0) despite the actual configuration.

  Workaround: Reset the interface by entering the **shutdown** command followed by the **no shutdown** command.

- CSCdm52953

  If you enable interleaving on a multilink interface, packets may be reordered when they are transmitted on the interface. The next packet to transmit might not be correctly selected from multiple conversational streams on the interface, and packets from the same stream could be rearranged. There is no workaround.

- CSCdm56000

  Virtual EXEC leaves unusable memory when you issue the **show tech-support** command. There is no workaround.

- CSCdm59077

  If you upgrade to Cisco IOS Release 12.0(3)T, AIP might not properly recognize the “Burst size in number of 32 cell bursts” option configured under the interface:

```
7513#conf t
7513(config)#int atm 1/0.1 point
7513(config-subif)#atm pvc 1 1 100 aal5snap 25000 10000 ? <b> <1-63> Burst size in number
of 32 cell bursts</b> inarp Inverse ARP enable oam OAM loopback enable <cr>
7513(config-subif)#atm pvc 1 1 100 aal5snap 25000 10000 <b>1</b> Invalid burst size of
1 cells requested: (ATM1/0): Not creating vc:1:1:100
7513(config-subif)# </pre>
```

  There is no workaround.

- CSCdm59722

  When using the virtual profile feature on a Cisco router that is also performing outbound calls, multiple calls might be placed even though the router is configured to make a single call to a destination.

  Workaround: Issue the **multilink max-links** command under the virtual-template interface to limit the amount of calls that are placed to the amount desired.

- CSCdm65381

  The process “ISDNMIB Background” is not releasing memory. The result is a loss in the router’s free memory. There is no workaround.

- CSCdm71874

  A Cisco router might enter “TEI_ASSIGNED” mode. In this case, a SABME poll is not answered by the router. There is no workaround.

- CSCdm74711

  A Cisco router will pause indefinitely if you enter the same map address in different permanent virtual circuits (PVCs) on the same subinterface. This action should not be attempted because it will cause the router to pause every time. There is no workaround.

- CSCdm77429

  A Cisco 3640 router might reload with a bus error when it is connected to a Frame Relay multicast-enabled network that reports the creation and then deletion of the multicast data-link connection identifier (DLCI). There is no workaround.

- CSCdm80712

  A Cisco AS5300 universal access server MICA module cannot call out in Japan if the **isdn calling-number** command is configured in the ISDN interface. There is no workaround.

XRemote

- CSCdm06301

  If you make a Telnet connection to a reverse XRemote port on an IOS device, and you do not provide a password when prompted, the IOS device will fall into an infinite loop and print repeated error messages to the Telnet client. The loop continues until the client disconnects the session. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(6)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(6). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdm42611

  MICA Technologies portware parameters are extended to support V110, along with other newly planned activities. The current Cisco IOS modem management MICA event handler does not handle event sizes beyond what the current version of Cisco IOS supports. If a new version of portware is added to an older version of IOS that does not support the new functionality, these event are dropped. There is no workaround.

- CSCdm50856

  The result of the **show modem** command on a Cisco AS5200 access server is different from the **snmpwalk** command of the cmInitialLineConnections variable defined in CISCO-MODEM-MGMT-MIB. There is no workaround.

Basic System Services

- CSCdk80230

  Certain Internetwork Status Monitor (ISM) NetView users can issue non-enable mode commands without router authentication. Users accessing the router through NetView must be authenticated through the NetView security methods, that might include RACF and SAF. Mainframe users can be restricted from issuing any router commands through the restriction of the RUNCMD within NetView. Users issuing enable mode commands must be authorized to issue this level of command through ISM, and must possess the enable mode password. If the router is controlled by TACACS+, the ISM user must have a TACACS+ user ID and password

- CSCdm33841

  The entity-physical table on a Cisco 7200 series router does not contain an entry for the network processing engine (NPE) card. There is no workaround.

- CSCdm41368

  A Cisco MC3810 multiservice access concentrator Ethernet output interface might enter a wedged state during which no traffic is transmitted from the router. This condition only occurs if a series of multiple or late collisions are detected on the Ethernet connection.

  Typically, it is not common to see a high number of late collisions on an ethernet environment. If you do, this might indicate extreme network utilization, ethernet network exceeding specifications, or possibly a bad port or cabling.

  The condition can be detected by issuing the **show interface ethernet 0** command on the Ethernet port. The symptom is that the output queue appears to be full (40/40), and output queue drops continue to increment. The following error message is displayed when the excessive collisions are detected:

  ```
  3810-analog-4#show interface ethernet 0 Ethernet0 is up, line protocol is up Hardware
  is PQUICC Ethernet, address is 0010.7b09.c62a (bia 0010.7b09.c62a) Internet address is
  172.16.173.5/26 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, reliability 255/255,
  txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set ARP type: ARPA, ARP
  ```

```
Timeout 04:00:00 Last input 00:00:09, output 00:01:45, output hang never Last clearing
of “show interface” counters 00:03:17 Queueing strategy: fifo Output queue 40/40, 42
drops; input queue 0/75, 0 drops

%PQUICC_ETHER-5-COLL: Unit 0, excessive collisions. Retry limit 15 exceeded
```

There is no workaround.

- CSCdm44772

  If the **show running-config** or **write terminal** commands are issued at the same time from two different virtual terminals (vtys), one session might finish before the other and damage a variable that the first session needs to use. This can cause the router to reload.

  Workaround: Do not issue the **show running-config** or **write terminal** commands at the same time from two different vtys.

- CSCdm45096

  A Cisco 1600 R router reloads with a bus error after you issue the **show line 1** command. There is no workaround.

- CSCdm45254

  If per-user configuration commands are downloaded from a AAA server, a Cisco AS5800 access server might reload or record spurious access errors.

  Workaround: Disable the per-user configuration commands or disable AAA authorization.

- CSCdm45535

  A Cisco 7500 series router can erroneously detect output stuck conditions. This condition causes interfaces to reset or perform CBus restarts for no apparent reason, causing all IPs in the router to reset. There is no workaround.

- CSCdm50432

  If you configure a Cisco MC3810 multiservice access concentrator Multiflex E1 interface for ATM, the interface might handle traffic-shaping parameters incorrectly. The generic cell rate algorithm (GCRA) schedules cells too aggressively, leading to usage parameter control (UPC) drops on the ATM switch even if double maximum burst size (MBS) values are provisioned. There is no workaround.

- CSCdm51380

  If more than one ipIcmpEcho probe is defined to begin at the same time, the responses can be mixed because the ID field in the ICMP header for both packets defaults to 1.

  Workaround: Change the ID field to a random number.

DECnet

- CSCdk23805

  When DECnet accounting is implemented, a Cisco router might reload due to a large number of connections. There is no workaround.

- CSCdm28939

  When you configure DECnet on a router, it is possible to specify an Address Translation Gateway (ATG) network number in the range 0 to 3. If the ATG-network-number is specified incorrectly when you configure an interface, the router might reload. If ATG-network-number is not required, it does not need to be specified and the problem does not occur. If ATG-network-number is required, use the following workaround.

  Workaround: Ensure that the ATG-network-number you specify when enabling an interface matches the one specified when DECnet routing is enabled globally (for example, **decnet** *1* **routing** *2.3* **interface** *ethernet 0/0* **decnet** *1* **cost** *5)*.

EXEC and Configuration Parser

- CSCdm58734

  The **padding** command on a line configuration is lost after the first successful connection. The command is reported when you issue the **sh configuration** command, but not when you issue the **sh running -config** command.

  Workaround: Reconfigure the **padding** command.

IBM Connectivity

- CSCdm11922

  If you use a data-link switching (DLSw) direct-encapsulation serial-link WAN with Ethernet LAN on one side and Token Ring LAN on the other, connections can only be established from the Token Ring side.

  Workaround: Raise the maximum transmission unit (MTU) of the serial WAN to approximately 1800 bytes.

- CSCdm30793

  A Cisco 7206 router that is configured for DLSw priority peers might reload with a bus error when running Cisco IOS Release 11.3(9)T. There is no workaround.

- CSCdm37638

  Some Cisco 4500 series routers and Cisco 4700 series routers with a 2-Port Token Ring Network Processor Module (NP-2R) might hang once a week (no matter the revision level of the motherboard), and display the following message:

  ```
  %SYS-2-INPUTQ: INPUTQ set, but no IDB
  ```

  Workaround: Issue the **lnm disable** command to temporarily correct the problem.

- CSCdm38759

  If a Router Switch Module (RSM) is configured with IBM spanning tree, and IP routing is disabled, it does not respond to a single-route or all-route ARP frame destined to its MAC address.

  Workaround: Disable IBM spanning tree on the RSM.

- CSCdm39124

  Console message flooding might occur when an XID3 loop occurs with an APPN in the router. The following messages are repeated for each iteration of the loop:

  ```
  %APPN-3-logcsCS_XXXXIP11_LOGMSG_01: CS - Sending Alert to MS, sense_code = 83E0001,
  proc_name = XXXXIP32, port_name = HMAC04, ls_name = @LS00289
  %APPN-3-logcsCS_XXXXIP11_LOGMSG_03: CS - Associated outbound XID data in alert (length
  ```

```
>= 29): %APPN-3-Error:
327307700000000000F7C100000000800001 0B5100050000000000007000E11F4C4C5C2E5D4E4F0F04BD5D
5C3C9D7F0F110380037110C0804F1F2F0F0F0F00908F0F0F0F0F0F0F01406C3C9E2C3D640C1D7D7D540D5
D561C4D3E4D90F0FC3C9E2C3D640C1D7D7D540D5D52207000000083E0001
%APPN-3-logcsCS_XXXXIP11_LOGMSG_05: CS - Associated inbound XID data in alert (length
>= 29): %APPN-3-Error:
326705D56F010000B00810000000000000010B410005B8000000000700103700231 10C0804F0F3F0F0F0F
00F06D4E240E2D5C140E2C5D9E5C5D90908F0F0F0F0F0F0F0131103100010F0F0F0F0F0F0F0F0F0F0F0
F00E0FF4C4C5C2E5D4E4F0F04BC3E3F5F6C6
```

Workaround: Avoid console logging.

- CSCdm40249

  A physical unit (PU) can not be brought online after you configure a new SDLC/DLSw pair.

  Workaround: Reload the router.

- CSCdm49573

  A Cisco router might reload with a bus error when you issue the **show dlsw circuit** command if there is a circuit with a local RIF of 18 bytes.There is no workaround.

- CSCdm50361

  DLSw peers might leak CLS connect request buffers.

  Workaround: Use a different peer type. This will free an outstanding connect request if additional requests are received while the first is still pending.

- CSCdm51010

  An advanced peer-to-peer networking (APPN) router might run out of memory due to unnecessary “lfsid” table expansion for some Dependent LU Requester (DLUR) links to downstream PU2.0s. This problem can occur after a DLUR takeover, or if the DLUR-PU had previously received a “dactpu not final use” message from the Dependent LU Server (DLUS). There is no workaround.

- CSCdm57363

  Synchronous Data Link Control (SDLC) test does not send or receive packets when peers are closed. There is no workaround.

- CSCdm59430

  In certain conditions, a Cisco router might reload in the “tcpd” routines or managed timer. There is no workaround.

Interfaces and Bridging

- CSCdk10376

  A Cisco router might reload in frf9_preComp(). This occurs most frequently when router traffic is heavy and memory usage increases causing a low memory condition.

  Workaround: Disable compression or use a different type.

- CSCdm38825

  Under certain conditions, source-route bridging (SRB) using a PA-4R-DTR Dedicated Token Ring port adapter might result in frames occasionally being bridged out of order. For protocols that are sensitive to the sequence of frames (such as Logical Line Control, type 2 [LLC2]), intermittent session loss might occur. There is no workaround.

- CSCdm40466

  You might lose connectivity on Inter-Switch Link (ISL) trunk subinterfaces if you configure a bridge group on one of the subinterfaces and then reboot the router. This is a Route Switch Processor (RSP)-specific issue and the problem is not seen on other platforms. Removing the bridge group does not resolve the problem.

  Workaround: Reboot the router after removing all the bridging and Bridge-Group Virtual Interface (BVI) statements.

- CSCdm40975

  Under certain conditions, a Cisco 7200 series router corrupts IP packets when using certain types of switching (for example, fast switching or Cisco Express Forwarding [CEF]) from an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) using bridging encapsulation and a Bridge-Group Virtual Interface (BVI). This condition only occurs if the sending bridge preserves the original cyclic redundancy check (CRC) in the packet.

  Workaround: Disable the appropriate type of switching.

- CSCdm41644

  A Cisco router running Cisco IOS Release 12.0 T might reload due to an overwrite issue in the BSS area when FDDI modules are used. There is no workaround.

- CSCdm46735

  A PA-4R-DTR port adapter might reset under the following circumstances:

  – A high rate of traffic is traversing the port (200 pps or greater).

  – The PA-4R-DTR port adapter is the active monitor of the physical Token Ring

  – An event on the ring occurs that forces the active monitor to purge the Token Ring

  When this problem occurs, the PA-4R-DTR port adapter resets, and the ring experiences a beacon.

  Workaround: Make sure the DTR port is not the active monitor on the Token Ring. This can be done by ensuring that the MAC address of the DTR card is not the highest MAC address on the physical Token Ring.

- CSCdm60960

  With the following input-type-list, a Cisco router does not respond to an Address Resolution Protocol (ARP) request.

  ```
  interface Ethernet0/0 ip address 10.10.13.1 255.255.255.0 standby 143 priority 110
  preempt standby 143 ip 10.10.13.254 bridge-group 1 bridge-group 1 input-type-list 201 !
  ```

  The router responds without it, and also responds if you add the line for ARP packets. You can ping the interface IP address but not the HSRP address.

  Workaround: Delete the input access lists on the bridge interface, or permit type 0x0806 in the access list.

IP Routing Protocols

- CSCdk83299

  The **lane client** command resets the address resolution protocol (ARP) timeout to the default value (four hours). After the **lane client** command is entered, any desired configuration of ARP timeout needs to be reentered, including immediately after reboot. There is no workaround.

- CSCdm44957

  Some IP fragments might be incorrectly filtered out by access lists. There is no workaround.

- CSCdm45873

  If you are redistributing OSPF routes into any other routing protocol, it does not include NSSA external routes. There is no workaround.

- CSCdm51483

  Executing the **show ip igmp group** command might cause a bus error reload if an IGMP entry is deleted during the command execution. This condition occurs intermittently. There is no workaround.

- CSCdm53317

  DNS replies that pass from “inside” to “outside” by way of Network Address Translation (NAT) might not be correctly NAT translated. There is no workaround.

ISO CLNS

- CSCdm45667

  Under certain circumstances, Cisco routers running Cisco IOS Release 11.3(9)T can stop receiving packets on interfaces. This happens when CLNS packets with an N-selector of 0x20 (the DECnet NSP protocol selector) are received by the router, and DECnet conversion has not been enabled or configured correctly. If this happens, the **show interface** command displays a full input queue and a number of dropped packets (for example, input queue 76/75, 122 drops).

  Workaround: Reload the router.

Miscellaneous

- CSCdk45491

  A 1-port Fast Ethernet network module (NM-1FE-TX) might fail to auto negotiate properly when connected through an SMF connector.

  Workaround: Manually set the speed to 100.

- CSCdk58186

  Half duplex should only be configured on an interface that is configured with a half duplex protocol (such as SDLC) or bisynchronous encapsulations.

  Workaround: Configure the interface for full duplex when not specifically running a half-duplex protocol. The interface command to do this is **full-duplex**.

- CSCdk66082

  Concurrent routing and bridging (CRB) of IP packets does not work when CEF and ISL are enabled. IP and ISL packets that are intended to be bridged are dropped as encapsulation drops by CEF.

  Workaround: Turn off CEF.

- CSCdm04861

  A race condition can exist between the processes that try to get connection status information from a VIP (and dropped packet information in Cisco IOS Release 11). A semaphore was added to prevent multiple processes from accessing the globals used at the same time. There is no workaround.

- CSCdm19457

  A Cisco 7500 router with a VIP or ESA-PA port adapter suffers from buffer starvation because of incorrect MEMD reservation. This problem is observed in Cisco IOS Release 11.2(7)P crypto images.

  RSPs with an ESA-PA allocate a MEMD buffer pool of size 32 bytes, which would never be used. This also leads to a reduced number of buffer headers available to other interfaces in the system. This leads to packet drops on other interfaces, even with moderate traffic load because of buffer starvation. For example, a router reserving an unused buffer pool would produce the following output:

  ```
  Router#show cont cbus MEMD at 40000000, 2097152 bytes (unused 612096, recarves 1, lost
  0) RawQ 48000100, ReturnQ 48000108, EventQ 48000110 BufhdrQ 48000130 (9 items), LovltrQ
  48000150 (16 items, 2016 bytes) IpcbufQ 48000160 (24 items, 4096 bytes) IpcbufQ_classic
  48000158 (8 items, 4096 bytes) 3570 buffer headers (48002000 - 4800FF10) pool0: 3206
  buffers, 32 bytes, queue 48000138 <======= Unused buffers pool1: 8 buffers, 256 bytes,
  queue 48000140 pool2: 217 buffers, 1536 bytes, queue 48000148 pool3: 78 buffers, 4512
  bytes, queue 48000168 pool4: 4 buffers, 4544 bytes, queue 48000170 slot1: VIP2, hw 2.4,
  sw 22.20, ccb 5800FF30, cmdq 48000088, vps 8192 software loaded from system
  ```

  Workaround: Remove the ESA-PA port adapter, if not used. Or, Upgrade your Cisco IOS software to Release 11.2(19)P, Release 11.2(19.01)P, Release 12.0(5.2), Release 12.0(5.2)PI06, or Release 12.0(5.5)T.

- CSCdm22032

  If you configure PPP encapsulation on an interface and then make that interface a member of a bridge group, the following messages will result:

  ```
  00:06:39: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:39:
  Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58
  602015E0 60556558 60553958 6021D034 6021D020 00:06:39: Fair Queue:packet not
  initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58 602015E0 60556558
  60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0
  , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback=
  601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not
  initialized properly: 0, 0 , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558
  60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0
  , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback=
  601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  ```

  Workaround: Remove bridging from the interface or turn off fair queueing.

- CSCdm28631

  If an encryption service adapter (ESA) is bringing up a large number of crypto sessions simultaneously (under conditions of stress), it might enter a race condition, or get a crypto initiation message wedged in the input queue of the interface processing the encryption. There is no workaround.

- CSCdm33429

  A Cisco AS5300 access server might experience a bus error under heavy loads that are caused by outgoing modem calls. There is no workaround.

- CSCdm34081

  An “ALIGN-1-FATAL” error is observed when the **copy tftp start** command is enabled while a configuration is loaded into NVRAM. There is no workaround.

- CSCdm36128

  A Cisco 3600 series router with 4T dial out might go down when you issue the **dialer dtr** command. There is no workaround.

- CSCdm37466

  Spurious accesses, router hangs, or router reloads can occur if you use fair queuing. There is no workaround.

- CSCdm38433

  A VIP configured for Distributed Cisco Express Forwarding (CEF) and Cisco Encryption Technology chassis (CET) might reload after you remove and reapply the crypto maps.

  Workaround: Apply the crypto maps one at the time and to go back to privilege mode between issuing the commands.

- CSCdm43653

  The process switching of Multiprotocol Label Switching (MPLS) packets received on an AAL5SNAP PVC subinterface fails. There is no workaround.

- CSCdm44057

  When running virtual profile, a Cisco 7500 series router continually resets the CBus. The following message is displayed:

  ```
  %RSP-3-RESTART: interface Serial4/0:1, output stuck
  ```

  Some time later, a reset occurs on the CBus. When you debug the CBus, you see the bus resetting which causes all attached controllers to loose connectivity. The only way to access the router is through the console port. There is no workaround.

- CSCdm44726

  Cisco IOS Release 11.3AA images do not support online insertion and removal (OIR) for ATM port adapters. If you OIR an ATM port adapter more than once, the router will hang. There is no workaround.

- CSCdm48870

  IPSec reports an incorrect MTU size. Crypto does not recognize an initial **ip mtu** command on an interface to which a crypto map has been applied. There is no workaround.

- CSCdm54169

  You cannot change the MTU size of a tunnel interface using software after Cisco IOS Release 11.3(9.2).

  Workarounds:

  – Use images between Release 11.3(5.1)T and Release 11.3(9.3) or Release 12.0(0.16) and Release 12.0(4.2).

  – Configure **ip mtu** on the tunnel interface before you configure **tunnel destination**. If **tunnel destination** is already configured, then unconfigure the destination, configure **ip mtu**, and then reconfigure the destination. You need to wait five seconds after removing the tunnel destination before issuing the **ip mtu** command. Once the workaround is issued, there should be no problems in the event of a router reboot as the **ip mtu** command is parsed before the tunnel destination.

- CSCdm55084

  When an SDR session is defined with a PA-A3 port adapter, a Cisco router might reload. There is no workaround.

- CSCdm55716

  An ATM subinterface might drop packets when Distributed CEF (DCEF) is disabled. This problem only occurs on subinterfaces created after DCEF is on, and then is turned off.

  Workaround: Enable, and then disable DCEF after creating a new subinterface.

- CSCdm55823

  Prior to Cisco IOS Release 12.0(6) tag forwarding fails. The **show adjacency** command shows that all of the tag adjacencies are marked incomplete. There is no workaround.

- CSCdm57097

  When there is traffic (ping) on the network, the IP cache entries (for one network reachable through two equal cost paths) are deleted (STALE RECURSIVE) and created every minute. There is no workaround.

- CSCdm57550

  A Cisco AS5800 access server might send incorrect port numbers to a radius server in AAA accounting. Regardless of which modem slot users get connected, the highest port number a user can obtain is 144, and there are multiple users with the same port number. There is no workaround.

- CSCdm57609

  A PA-A2 port adapter might cause memory corruption if you use SVCs with an ARP-server when you shut down the interface. There is no workaround.

- CSCdm58776

  If a router running CET encryption has many connection setup attempts happening at once, some might time out prematurely. Also, some connection setup attempts might not setup properly. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdk04507

  Routers running IPX and EIGRP with Cisco IOS Release 11.2 or greater can reload when there are frequent interface up and down transitions. This problem is most common with dial-up interfaces.

  Workaround: Disable IPX and EIGRP.

- CSCdm46556

  In Cisco IOS Release 11.2, if SAP passive update is configured on an interface, the services learned on that interface never age out of the table. In Release 11.3 and later, this also occurs on networks learned on RIP passive interfaces. There is no workaround.

Wide-Area Networking

- CSCdj39383

  A Cisco router with over 180 data-link connection identifiers (DLCIs) can not boot properly due to excessive console log messages related to the startup of Frame Relay PVCs. There is no workaround.

- CSCdm01618

  When a Cisco router is functioning as an X.28 packet assembler/disassembler (PAD), it should send an X on to the data terminal equipment (DTE) as soon as it enters the data transfer mode if parameter 5 is set to 1. The PAD does not. There is no workaround.

- CSCdm30090

  When a Cisco router is operating as an X.25 switch, and forwards an X.25 call containing certain facilities not interpreted by the router, the facility values might be corrupted. The problem occurs most often when the call cannot be forwarded immediately (for example, when using X.25-over-TCP) with heavy traffic. The affected facilities include any local facilities and the Charging Information facility. There is no workaround.

- CSCdm32801

  In an NFAS group with a primary and a backup D-channel, fast busies might occur depending on the failure. If the T1 with the primary D-channel is shut down or fails, and the backup D-channel comes into service, call routing to a modem in the access server is successful. If the T1 with the primary D-channel remains in an up condition, but the primary D-channel fails, the backup D-channel comes into service and call routing fails for B channels on the T1 that contained the primary D-channel. Users dialing in get fast busies in this scenario. However, calls on all the other NFAS members, including the T1 with the backup D-channel, are successful. There is no workaround.

- CSCdm34846

  A Cisco router might reload when the **ip rtp header-compression** command is deconfigured and encapsulation is changed from PPP to Frame Relay. There is no workaround

- CSCdm36123

  A Cisco router might reload with a SegV exception if dialer rotor best is configured, or if deb dialer is started once traffic triggers a call. There is no workaround.

- CSCdm37653

  Reliable PPP can cause intermittent reloads when used with WFQ.

  Workaround: Disable Reliable PPP or WFQ.

- CSCdm38291

  Dialer watch backup does not dial after the backup interface times out. There is no workaround.

- CSCdm41090

  A Cisco 4500 series router might experience a memory leak. When a remote sites go down, or when an ISDN link drops, the router repeatedly attempts to dial the remote site. If the connection is not established, the router keeps dialing, eventually runs out of memory, and hangs.

  Workaround: Reboot the router.

- CSCdm43734

  When dialer watch uses an ISDN connection for the backup link, and the ISDN connection fails to connect during the connection timeout, and there are multiple dialer maps specifying the destination IP address corresponding to the watched route, dialer watch fails to retry the secondary connection, even if the watched route becomes operational and then fails again.

  Workaround: Code only a single dialer map command for the secondary interface going to the watched IP address.

- CSCdm48047

  A Cisco 4000 family router might reload if you configure LECS, LES/BUS, and LEC on the router. There is no workaround.

- CSCdm48450

  When stac compression is enabled on RSP routers configured for bridging with HDLC encapsulation, the router is unable to pass traffic.When checking the start of the HDLC packet to determine if it is a bridged packet board, encapsulations are not taken into account. Because of this, HDLC_BRIDGECODE is not read correctly.

  Workaround: Disable compression.

- CSCdm54100

  Autoselect functionality does not exist in Cisco IOS Release 12.0 prior to Release 12.0(6). There is no workaround.

- CSCdm57650

  In Multi-chassis MLP stack group, when two stack group member cross project MLP link interfaces. One of the stack group members might crash. There is no workaround.

- CSCdm58462

  When LANE clients are configured with more than 14 HSRP groups per subinterface, along with Multiprotocol over ATM (MPOA), a Cisco router might reload due to insufficient buffer space for carrying all the HSRP MAC addresses. There is no workaround.

- CSCdm59077

  If you upgrade to Cisco IOS Release 12.0(3)T, AIP might not properly recognize the “Burst size in number of 32 cell bursts” option configured under the interface:

  ```
  7513#conf t
  7513(config)#int atm 1/0.1 point
  7513(config-subif)#atm pvc 1 1 100 aal5snap 25000 10000 ? <b> <1-63> Burst size in number
  of 32 cell bursts</b> inarp Inverse ARP enable oam OAM loopback enable <cr>
  7513(config-subif)#atm pvc 1 1 100 aal5snap 25000 10000 <b>1</b> Invalid burst size of
  1 cells requested: (ATM1/0): Not creating vc:1:1:100
  7513(config-subif)# </pre>
  ```

  There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(5)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(5). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdm09417

  A Cisco AS5200 access server might not be able to dial out using channel associated signaling (CAS). This condition occurs intermittently. There is no workaround.

- CSCdm21149

  On a Cisco AS5800 access server, modem PPP autoselect and plain character-mode login can fail. No response is received from the server (Cisco AS5800) modem, even though the modem connects successfully. There is no workaround.

- CSCdm21330

  If you configure a maximum transmission unit (MTU) that is different from the serial interface default value that is created using a channelized group on an E1 four-port controller, the following error message is generated:

  ```
  %DSX1-3-M32_MEM_ALLOC: Munich 32 channel memory allocation error
  ```

  The serial interface is then put in an administrative shutdown state. There is no workaround.

AppleTalk

- CSCdm35802

  When running **test appletalk**, the command-line interface (CLI) can hang during **nbp lookup** or **nbp confirm** tests. This occurs when the user specifies network-visible entity (NVE) names with null strings for the “object” or “type.” The commands in the following example cause the CLI to hang, but allow other router functions to continue:

  ```
  router# test apple
  router(atalk test)# nbp lookup ?
  LINE <object>:<type>@<zone>
  router(atalk test)# nbp lookup :laserwriter@bpath
  ```

  There is no workaround.

Basic System Services

- CSCdj93398

  A Cisco router might display the following error message:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 279DC -Process= "traffic_shape",
  ipl= 6, pid= 41 -Traceback= 317DAEC 318353A 31B116
  ```

  There is no workaround.

- CSCdk17135

  Fast switching is not functional between 100Vg-AnyLAN and a PA-A1 port adapter. There is no workaround.

- CSCdk48674

  A Cisco 1600 series router is not able to receive Ethernet frames at wire speed. This causes the Cisco 1600 series Ethernet driver to miss packets. The problem appears when a Windows 95 or Windows NT machine joins more than 60 groups. The IGMP replies it sends are at wire speed, so multicast groups are lost at the Cisco 1600 series router.

  Workaround: Configure static multicast groups.

- CSCdk54265

  When you upgrade a router to Cisco IOS Release 11.1(20)CC, there is a significant change in the amount of time and CPU usage required to process network management requests. After the upgrade, the CPU is utilized between 90 to 99 percent, and the process runs for over 1 hour.

  The problem occurs when the demand poll (for example, HP OpenView [HPOV] or a NetMon process) walks the routing table by way of Simple Network Management Protocol (SNMP). This polling walks other things as well, such as Address Resolution Protocol (ARP) tables and interface descriptor blocks (IDB). However, these take less than 10 seconds and have little affect on the processor.

The default priority of the SNMP process was changed (from medium to low) in early releases of Cisco IOS Release 11.1 to allow the scheduler to service other processes while SNMP is running. This change makes SNMP interference with normal routing functions rare, because packet forwarding and routing are medium- or high-level processes. The result is that SNMP relinquishes the processor if required. Conversely, SNMP uses all of the available processor to complete this task.

Workaround: Disable routing table walking using an SNMP view statement in the router configuration. This might hinder the discovery of unnumbered links in the network, as well as increase the time of discovery.

- CSCdk54312

  Online insertion and removal (OIR) on a Cisco 7500 series router running a Cisco IOS Release 12.0 release might cause “OUTPUT STUCK” and “CYBUS COMPLEX RESTARTS” errors. There is no workaround.

- CSCdk59010

  If you use reverse Telnet to a binary Telnet port with RFC-2217 comport extensions, and if you make multiple successive dialouts from within the context of the single Telnet session, the Cisco IOS Telnet server prematurely sends a “FIN” to the RFC-2217 client after several outgoing calls. The Cisco DialOut client sees the following popup window:

  ```
  Cisco DialOut Utility Received message from Cisco Dialout Port: COM4 Server: COM4 >
  172.16.135.12:7001 Return code: 10053 Message: Unexpected Network Error [ OK ]
  ```

  There is no workaround.

- CSCdk63484

  In certain circumstances, the IPX EIGRP topology table and routing table do not show entries for routes that are showing on other IPX EIGRP neighbors. If you issue the **debug ipx eigrp** command, the affected router shows that the updates are being received, but the entries are never added to the topology table.

  Workaround: Enable IPX RIP/SAP to allow all routers to see all IPX routes.

- CSCdk72065

  The correct buffer size should be determined before zeroing the buffer. There is no workaround.

- CSCdk75315

  In some cases, error messages are generated by RSP routers with VIP cards. The error messages are generally benign, indicating temporary “out of memory” situations. The memory is then recovered. There is no workaround

- CSCdk80074

  Initializing a Basic Rate Interface (BRI) that is connected to a Siemens HICOM PABX fails. This leaves the layer 1 status in “ACTIVE_ErrorInd.” There is no workaround.

- CSCdk93431

  When authorizing with TACACS+ on an IPX dialup, the access IPX list is not accepted during the authorization process.

  Workaround: Downgrade to Cisco IOS Release 11.3 (5).

- CSCdm02753

  A Cisco 7200 series router with a data encryption service adapter (ESA) card might periodically reload. There is no workaround.

- CSCdm11467

  When utilizing Network Time Protocol (NTP) private mode and control type messages for remote query, a router might reload or you might see traceback messages. There is no workaround.

- CSCdm13269

  If you configure the 128-kbps leased line on a Cisco 1003 router, and the router runs Cisco IOS Release 12.0(3), the following message might appear when the router boots:

  ```
  ASSERTION FAILED: file "../src-36/quicc_driver_lib.c", line 215
  ```

  In this situation, the feature does not work. There is no workaround.

- CSCdm13937

  A router might reload with a software-forced error if syslog SNMP traps are enabled and no additional dynamic memory is available on the router. The following message is displayed:

  ```
  %SYS-2-FREEBAD: Attempted to free memory at DEADBEEF, not part of buffer pool
  %SYS-2-FREEFREE: Attempted to free unassigned memory at 61955EE4, alloc 60655D14,
  dealloc 60650288 %SYS-6-BLKINFO: Attempt to free a block that is in use blk 61955EBC,
  words 62, alloc 60655D14, Free, dealloc 60650288, rfcnt 0
  ```

  There is no workaround.

- CSCdm16625

  The **write network** command does not work if you issue the **tftp-source interface** command first. There is no workaround.

- CSCdm17336

  The Hewlett-Packard (HP) Probe subsystem is not included in any Cisco 1600 series images in any Cisco IOS releases. There is no workaround.

- CSCdm21161

  If you use a VIP CE1/TE1 interface you might see "RSP-3-INVRTN" or "RSP-3-NORESTART" errors, followed by the logging of much debugging information and a switching complex restart. There is no workaround.

- CSCdm32905

  A Cisco MC3810 multiservice access concentrator running Cisco IOS Release 12.0(3)T1 fails to remove a directly connected route from the routing table when the interface for the network goes into a "line protocol down" state. This should not be an issue unless you have another route to the network. There is no workaround.

DECnet

- CSCdk62414

  Under certain conditions, DECnet does not send triggered routing updates after an adjacency comes up. If periodic routing updates are sent out frequently (the default frequency being 40 seconds), this is not an issue because an update gets sent out in a short time and routes are learned. However, if the routing update timer has been configured to be a large value, routes might not be learned for a long time.

  Workaround: Configure a smaller value for the routing update timer.

EXEC and Configuration Parser

- CSCdj92253

  A Cisco router might unexpectedly restart if multiple connections are made from a virtual terminal, and one of the connections is closed due to a session timeout while another connection is blocked from sending data due to being flow controlled. There is no workaround.

- CSCdm15221

  If you configure the asynchronous interface of any Route Switch Processor (RSP) chassis with a VIP2 or VIP2-50 in slot 0, with any port adapter of any kind, the proper parsing of interfaces in either port adapter in the VIP in slot 0 will be prevented.

  Workaround: Deconfigure any asynchronous interface, write the configuration to NVRAM, and reload the router. This defect is in all Cisco IOS Release 12.0 images. Another choice is to move any VIP from slot 0 to another slot.

- CSCdm32506

  A bus error might occur when you issue the show running-configuration command. There is no workaround.

- CSCdm33057

  A MICA modem line with flow-control software does not properly respond to an "XOFF" received from the modem if the line is running an outbound Telnet session. Output from the **show line** command shows that the line is in the "Waiting for XON" state. Although the Cisco IOS software should wait for an "XON" before sending data out the line, it does not. There is no workaround.

- CSCdm39355

  A Cisco router might reload during command completion if the length of the entire command after completion exceeds PARSEBUF.

  Workaround: Do not allow command completion if it exceeds PARSEBUF.

IBM Connectivity

- CSCdk51086

  When QLLC is used as a transport mechanism for SNA traffic, X.25 might get stuck in "Receiver not Ready" (RNR) when the input queue is full.

  Workaround: Increase the capacity of the input queue to 1000 packets.

- CSCdk81731

  When **DLSw icanreach** is configured on a router, the filter should be applied on source SAP for the frames going out to remote peers, and on the destination SAP (in the remote peer) for the frames going to the peer on which **DLSW icanreach** is configured. The filter is applied to both source SAP and destination SAP in both DLSw peers. There is no workaround.

- CSCdm09164

  A Dependent Logical Unit Requester (DLUR) router might reload with the following stacktrace:

  ```
  RA: 0x6070294C[mu_processor(0x60702630)+0x31c] RA:
  0x60702F84[remote_path_control(0x60702e50)+0x134] RA:
  0x607044D0[pc_mainline(0x60703d60)+0x770] RA: 0x606FF3B8[xxxpcasm(0x606ff000)+0x3b8]
  ```

  There is no workaround.

- CSCdm10184

  A Cisco router might send an information frame with the poll bit set and then send a relative rate (RR) with the poll bit set. This causes the end station to send a window of information frames twice. There is no workaround.

- CSCdm12293

  In Cisco IOS Release 12.0(3.5), Release 11.3(8.5), and Release 11.3(9), features that use SDLC do not work. There is no workaround.

- CSCdm13939

  If you use a combination of DLSw with Ethernet 80d5 frame processing and Cisco IOS Release 11.3, DLSw will not forward response Logical Link Control (LLC) protocol data units (PDUs).

  Workaround: Hardcode all the service access points (SAPs) with the **source-bridge sap-80d5** command.

- CSCdm14582

  A router running Advanced Peer-to-Peer Networking (APPN) might reload with a SegV exception. The following stacktrace is created:

  ```
  0x606C30CC:process_purged_ips(0x606c3060)+0x6c 0x606C3024:hsp04(0x606c2dd0)+0x254
  0x606C2DAC:hsp00(0x606c2d80)+0x2c
  ```

  There is no workaround.

- CSCdm14583

  If a Berkeley Internet Name Domain (BIND) arrives at a Cisco network node/DLUR, and is destined for a secondary logical unit (SLU) beneath that DLUR, and the primary logical unit (PLU) name is not qualified, you reject the BIND with sense code 0x0835001B. The “1B” is the offset into the BIND of the PLU name field. There is no workaround.

- CSCdm19563

  If you use data-link switching (DLSw) or Qualified Logical Link Control (QLLC) with PVC configured, when you upgrade to Cisco IOS Release 11.3(8), the VMAC generated by QLLC is set to 0000.0000.0000. In the lab environment the circuit connected properly, but this might not be the case if an access list is implemented.

  Workaround: Use the latest release of Cisco IOS Release 11.2.

- CSCdm20764

  An Advanced Peer-to-Peer Networking (APPN) router might create a topology storm over the status of a Branch (Extender) transmission group (TG). The router’s Branch Awareness function (APPN option set 1120) is inadequate. There is no workaround.

- CSCdm21529

  The Channel Port Adapter (CPA) does not recover from a fatal error reload. This requires the user to manually reload the microcode for this card. If the user enters the **show running-config** or **write terminal** commands while in this mode, the console will lock up and display the “SCHED-3-THRASHING” error message.

  Workaround: If the card does not restart after a CPA fatal error, issue a **microcode reload** [*ecpa* | *pcpa*] **slot** *n* command to reload the microcode for the problematic card. If you get the “SCHED-3-THRASHING” error message, Telnet to the router on a different vty and perform the microcode reload there.

- CSCdm26717

  APPN/DLUR experiences corruption when the total number of PUs and LUs approaches 8000. This problem is typically preceded by spurious memory accesses. The resulting failures are variable, such as a corrupt CVx'60' on DLUR-DLUS flows, SESSEND failures from DLUR with sense code 0x1014023D, and PUs and LUs becoming stuck in "Stopping" state. There is no workaround.

- CSCdm27224

  When static NetBIOS name cache entries are defined using the **netbios name-cache** configuration command, issuing a subsequent **show netbios name-cache** EXEC command will produce traceback messages and might cause a Cisco router to unexpectedly restart. There is no workaround.

- CSCdm33134

  In a DLSw environment where there are many unpaced SNA frames (for example, using DSPU with many LUs defined), high CLS congestion can result in a "ZWO" being sent followed by a "RWO" without waiting for an FCA response. This will cause the circuit to hang at Cw:0.

  Workaround: Clear the circuit.

- CSCdm37870

  An APPN router running HPR might reload with the following stack trace:

  ```
  Enter hex value: 0x7D910C 0x7D910C:__start(0x60008000)+0xa07d110c Enter hex value:
  0x608EFA20 0x608EFA20:Qfind_front(0x608efa10)+0x10 Enter hex value: 0x608342F8
  0x608342F8:lrp10(0x608340f8)+0x200 Enter hex value: 0x60832E04
  0x60832E04:lrp02d(0x60832d64)+0xa0 Enter hex value: 0x60832750
  0x60832750:lrp00(0x60832548)+0x208 Enter hex value: 0x60250D6C
  0x60250D6C:r4k_process_dispatch(0x60250d58)+0x14 Enter hex value: 0x60250D58
  0x60250D58:r4k_process_dispatch(0x60250d58)+0x0 Enter hex value:
  ```

  There is no workaround.

Interfaces and Bridging

- CSCdj90833

  When an eight-ISDN B-channel Multilink PPP bundle is configured by way of a dialer rotary group and a dialer interface on a Cisco 7206 router with ATM port adapters, the router reloads periodically every one to three hours. Turning off Multilink PPP bypasses the problem at the cost of performance. This problem also exists when doing fast switching from other tunneling protocols to the ATM Lite. There is no workaround.

- CSCdk67709

  Multilink PPP interleaving causes a delay in outbound traffic on RSP platforms. There is no workaround.

- CSCdk88242

  Frame Relay traffic shaping does not work on Frame Relay subinterfaces of a PA-2CE1 channel-group port adapter installed on a VIP2.

  Workaround: Configure Generic Traffic Shaping (GTS) on Frame Relay subinterfaces.

- CSCdk92089

  If you have Integrated Routing and Bridging (IRB) configured on a Cisco 4500 router with two Token Ring interfaces (0 and 1) on bridge 1, when a PC is connected to interface 0 everything works fine (the MAC is on the bridge table and pings are successful). However, as soon as you change the connection to interface 1, the MAC does not show up on the bridge table and pings are not successful. There is no workaround.

- CSCdm13938

  If you use transparent bridging on a Catalyst 8540 multiservice ATM switch router, and attempt a BOOTP, the "RARP" message from the client never reaches the server if the Bridge-Group Virtual Interface (BVI) is defined. As soon as you remove the BVI126 interface, the "RARP" goes through the Catalyst 8540, but the client will not finish booting. There is no workaround.

- CSCdm16052

  In Cisco IOS Release 11.3(8.5)T, the RSM and RSP platforms that use a VIP2/PA-4R IBM2692 port adaptor will potentially ignore non-RIF Token Ring packets. This condition occurs because the VIP Token Ring driver incorrectly classifies these packets as runts and drops them. This is a regression and was introduced by CSCdk64195. There is no workaround.

- CSCdm16154

  A VIP port adapter that is configured for encapsulation ISL 99 experiences a 30 to 70-percent packet loss when pinging a host that is located on the same VLAN off of a directly connected switch. The switch is configured to forward VLAN 1 -1005. The issue seems to be traffic related (nature of the traffic, not amount), because the addition of certain VLANs on the switch trunk side triggers it.

  Workaround: Use Cisco IOS Release 12.0(3.3)S instead of Release 12.0(3.5)S, or clear the trunk to contain only VLAN 99.

- CSCdm19165

  A bridge filter might not filter out all the MAC addresses it should filter. There is no workaround.

- CSCdm36454

  A Cisco 7200 series router running Cisco IOS Release 12.0(3.5) or later images will display the following error message when a Fast Ethernet port adapter is removed from the chassis:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=0, count=0
  ```

  There is no workaround.

IP Routing Protocols

- CSCdk09082

  Some types of incorrectly formed DNS packets might cause a Cisco router to reload. There is no workaround.

- CSCdk78108

  When using two EIGRP processes on a router, a directly connected network might end in an internal loop after the link associated with that network goes down and up. This will result in a routing failure to that network. There is no workaround.

- CSCdk84841

  When you configure an X.25 line as a passive interface for OSPF, the line might stay in an OSPF "down" state after a line flap, even though the line protocol is up. You can check the OSPF state in the output of the **show ip ospf interface** command. As a result, this line's network number will not be advertised by OSPF.

  Workaround: Do not to make this interface passive for OSPF.

- CSCdm02740

  When an interface with **ip cgmp** configured is deleted, some data structures are not properly cleared. If the interface is later recreated and **no ip cgmp** is configured, the router will reload.

  Workaround: Configure **no ip cgmp** before deleting the subinterface.

- CSCdm05636

  CPU utilization can be too high due to the number of NAT entries in the NAT table. There is no workaround.

- CSCdm13956

  ICMP redirects can overwhelm process switching.

  Workaround: Clear IP redirect or reload the router.

- CSCdm25188

  A Cisco router might reload if a badly formed h323/h225 packet is processed by NAT. There is no workaround.

- CSCdm28898

  ARP to a router fails on the serial interface when bridging is enabled after a router is reloaded. This condition occurs with Cisco 2500 series routers running Cisco IOS Release 11.2(17) and Release 12.0(3.7).

  Workaround: Remove the IP address on serial interface and reenter it.

ISO CLNS

- CSCdm28035

  If a Cisco router originates multiple link-state packets (LSPs), the fragments might not be correctly purged from the neighboring LSPDB. The problem is only seen with "authentication;" that is, if **domain-password** [*xxx*] is configured. There is no workaround.

Miscellaneous

- CSCdj89070

  The command **show crypto card** on a Cisco 7500 series router does not return any information. The command should provide output similar to the following:

  ```
  Router# show crypto card 1 Crypto card in slot: 1 Tampered: No Xtracted: No Password set: Yes DSS Key set: Yes Router#
  ```

  To verify that the card is recognized by the software, use the **show diag** or **show crypto engine brief** commands. There is no workaround.

- CSCdk12480

  A VIP encryption engine does not successfully negotiate an encryption connection with an encryption peer if traffic that needs to be encrypted or decrypted by the VIP is received at initialization time (such as after a reload or an OIR). After the VIP has reinitialized, the **show crypto connection** command shows an ID of "0." However, **show crypto map** will show a negative connection ID.

  Workaround: Clear the ID manually with the **clear cryp conn** [*connection_ID*] [*vip_slot #*] command. The router will display an error message, but it will successfully negotiate a crypto connection.

- CSCdk27245

  An ATM receiver might stop receiving frames after you remove a PVC from a shutdown ATM subinterface, or if you remove an ATM subinterface.

  Workaround: Clear the ATM interface.

- CSCdk33027

  If two encryption access lists are different, but each has the same IP address as the lowest numbered IP address in the ACL sources, and the same lowest numbered IP address in the ACL destinations, they will be erroneously treated as the same encryption session. This results in only one of the two encryption sessions being used at any one time. The one encryption session that is active might not work reliably. There is no workaround.

- CSCdk34543

  Encryption does not work properly when a Cisco 7500 series router is used in combination with a VIP2-40, and a PA-2CE1 (or PA-CE1) port adapter if the channelized E1 interface is configured for Frame Relay. This problem is related to distributed services, only the channelized E1 port adapters on the VIP2-40 are affected.

  Workaround: Use a VIP2-15 instead of a VIP2-40.

- CSCdk50386

  The **show syscon mibpoll** command displays no data if the community strings on the system controller manager and the system controller agent are different.

  Workaround: Make the strings on the system controller manager and the system controller agent identical.

- CSCdk55881

  When Distributed Cisco Express Forwarding (DCEF) is enabled on Internet routers, the counters on access lists are not incremented. There is no workaround.

- CSCdk69415

  An RSP-based router running the rsp-isv56-mz.112-15a.P Cisco IOS image stops passing IP traffic destined through two FDDI port adapters when the traffic is encrypted and decrypted on a VIP2-40.

  Workaround: Reload the microcode. The problem might reoccur.

- CSCdk73370

  A Cisco 3600 series router with a Multi-BRI (MBRI) cannot forward transparent bridging packets on the BRI leased 64-kbps line.

  Workaround: Downgrade to a Cisco IOS Release 11.2 image.

- CSCdk75285

  When a Certificate Revocation List (CRL) size is larger than 2 KB, the router might reload.

  Workaround: Have the server issue a smaller CRL.

- CSCdk75500

  The R2 signaling timeslots (or channels) on a Cisco AS5800 access server might lock up every two weeks.

  Workaround: Delete the CAS-group configuration item then put it back, or reload the access server.

- CSCdk76039

  On a Cisco 7500 series router that uses Multilink PPP (MLPPP) and Voice over IP (VoIP), the VIP code might consume packets too quickly and disable the VoIP MLPPP interleaving feature when WFQ is used on RSP. This condition causes speech quality to be degraded. There is no workaround.

- CSCdk77410

  The Cisco 4700 low-speed interface NP2T16S pin 24 TxCE has no signal output. This causes problems (for example, a “line protocol is down” message) when a DCE enables dce-terminal-timing. There is no workaround.

- CSCdk79100

  When CEF switching becomes disabled due to low memory conditions, an interface’s packets managed by CEF switching are dropped due to unresolved adjacencies. However, those managed by process-level are successfully routed. This results in a switching degradation of about 50 percent until CEF is reinitiated on the router.

  Workaround: Reenable CEF.

- CSCdk79570

  When you use a Cisco 4500 or Cisco 4700, a ping over Token Ring LANE cannot contain more than 4480 bytes. There is no workaround.

- CSCdk81331

  On Cisco 7500 series routers and Cisco 12000 series routers, tag switching might not function properly if Distributed CEF (DCEF) is enabled. This is because the tag forwarding table might not be properly created on the VIP linecards.

  Workaround: Disable DCEF using the **ip cef** configuration command.

- CSCdk84296

  IPSec reports an incorrect MTU size. Crypto does not recognize an initial **ip mtu** command on an interface to which a crypto map has been applied.

  Workaround: Turn off the Don’t Fragment (DF) bit on packets going into an IPSec tunnel, then remove the **ip mtu** command from the interface definition and reboot the router. After the router has rebooted, add the **ip mtu** command back to the interface definition.

- CSCdk85615

  On a Cisco 3640 router, there is no way to configure MICA modem lines for “dialout only.” The **modem dtr-active** command fails with a “NO DIALTONE” error message. There is no workaround.

- CSCdk91758

  A Cisco 3620 router running Cisco IOS Release 11.3.(6)T might reload when you use RADIUS to enable AAA authentication. This is not a problem with Cisco IOS Release 11.2. There is no workaround.

- CSCdk92265

  If online insertion and removal (OIR) is performed on a DMM card, autoselect fails. There is no workaround.

- CSCdk93438

  A VIP controller on a Cisco 7500 series router might hang when encryption is used. This condition is intermittent.

  Workaround: Reload the router.

- CSCdk93483

  If voice traffic is process-switched (for example, when using RTP Header Compression), the execution of certain EXEC commands on the router (for example, the **show running-configuration** command), can have an adverse effect on the quality of voice calls during the execution of the command when it is competing with voice packets for CPU time. There is no workaround.

- CSCdm01005

  Committed Access Rate (CAR) fails to forward traffic when fragmentation is required and fast switching is in use.

  Workaround: Disable fast switching.

- CSCdm03148

  If you have a Cisco 7513 router with up to six channelized T3 cards, with many serial interfaces, and you have recently upgraded from Cisco IOS Release 11.1(21)CC2 to Release 11.1(23)CC, the **copy run start** command might take longer to execute, and performance problems might occur with the router. SNMP responses can be noticeably slowed, and serial lines can see a line protocol drop. This condition occurs when DCEF is enabled globally, but disabled on the VIP2 interfaces.

  Workaround: Remove CEF from the router, or remove CEF distributed and apply IP CEF. You can also enable DCEF.

- CSCdm04449

  OAM TX might be dropped.

  Workaround: Use a release of Cisco IOS software that is older than the following releases: Cisco IOS Release 11.3(05)DB0.3, Cisco IOS Release 11.3(06.06)DB0, Cisco IOS Release 12.0(2.4), Cisco IOS Release 11.3(7.2)AA, Cisco IOS Release 12.0(2.4)T, Cisco IOS Release 12.0(2.5)S, Cisco IOS Release 11.1(23.02)CC, Cisco IOS Release 12.0(2.5)PI, or Cisco IOS Release 12.0(02.05).

- CSCdm06832

  A Cisco 1700 series router might inadvertently reload with SegV exception. There is no workaround.

- CSCdm07890

  A relay IP address is not correctly completed when you configure DHCP proxy under virtual templates. There is no workaround.

- CSCdm08139

  If Cisco a router runs Cisco IOS Release 11.3(8)T1 56-bit Encryption, and is configured to run IPSec over Frame Relay, a point-to-point interface fails. The packets from the source IP address are dropped when the router configured for IPSec. There is no workaround.

- CSCdm08164

  When running Cisco IOS Release 12.0(3) on the Cisco 7200 series, it is possible to see periodic interface resets on DS3-speed links under high interface utilization. This can result in a loss of keepalives and output drops. There is no workaround.

- CSCdm08728

  Cisco router running Cisco IOS Release 11.3(6)T can experience unexpected system restarts when configured with the crypto IPSec commands. There is no workaround.

- CSCdm09652

  In certain topologies, HSRP with RSMs and Token Ring LANE in a Cisco Catalyst 5000 series switch does not work properly if the LANE connections get interrupted. Connectivity does resume after a timeout, depending on the end systems used. There is no workaround.

- CSCdm10475

  If you reload a Cisco 3600 series router while the PRI D channel is in "STANDBY" or "SHUT" mode, layer 1 can get stuck in "ACTIVATING" mode. The following error message is displayed:

  ```
  ISDN Se2/0:23: Could not bring up interface
  ```

  Workaround: Reload the router, then issue the **backup interface** command.

- CSCdm11990

  DMM modem cards might fail. When the failure occurs, the modem is allocated to an incoming call and the modem trains up, but no data is received from the client. There is no workaround.

- CSCdm12319

  After an undetermined period of time (which can vary depending on whether CET or IPSec is being used and the length of the key timeouts), encryption might stop working. The symptoms include a lack of debugs from one of the encryption modules, as well as an interruption of the flow of encrypted data. Data that should be encrypted is no longer sent because the IPSec negotiation is never completed. This does not affect nonencrypted data because it continues to be switched by the router. Only data that would normally be encrypted will not be sent. There is no workaround.

- CSCdm13977

  When you use the **atg ip default-route** command, a tag for the default route is built and traffic arrives on a virtual circuit (VC), but the traffic is not forwarded by the router. The traffic is only reported by the **show atm vc** command but not in the **show interfaces stats** or **show interfaces atm** [*slot*/*port*] commands. There is no workaround.

- CSCdm15174

  If you load and run Cisco IOS Release 12.0(3.5) images from any code branch (for example Release 12.0(3.5), Release 12.0(3.5)T or Release 12.0(3.5)S) on RSP platforms, you might find that the boot variables are not properly set and that reloads of these platforms might not occur as planned from the configuration written to NVRAM. This is determined by an examination of the boot variables using the **show bootvar** command. The following is an example of the output associated with the **show bootvar** command:

  ```
  nu-blab-gw1# show bootvar

  BOOT variable = slot1:rsp-jsv-mz.120-3.6,1;slot1:rsp-jsv-mz.120-2.7,1; CONFIG_FILE
  variable = BOOTLDR variable = slot0:rsp-boot-mz.120-2.7 Configuration register is 0x2
  ```

  If the boot variable is not as planned, it is suggested that customers running any RSP Cisco IOS Release 12.0(3.5) image wait for images that have the fix for this defect.

Workaround: Achieve control of the router from the console, (not from a vty connection) and perform the following steps, assuming the corrected image resides in Flash memory (bootflash, slot0, or slot1):

a) router# **configure terminal**

b) router(config)# **config-register 0x0**

c) Press **Ctrl-C**.

d) Reload the router

e) router> **rommon** > **b slot1**: new image (The “new image” is the name of Cisco IOS image, assuming it resides in slot1.)

f) After the reload directly from Flash memory, perform a **write memory** to correct the boot variable images until a fixed image is available.

- CSCdm17500

  In various Cisco IOS Release 12.0 releases, the network-clock cannot be retrieved from the CBR interface of a PA-A2 port adapter even though the CBR interface is up. It will be declared down by the **show network-clock** command. There is no workaround.

- CSCdm18330

  If a Cisco platform that uses asynchronous ports is sent a BREAK sequence, closely followed by additional data, the line can stop sending output unless manual intervention occurs. This condition can occur until an automated script sends a Telnet BREAK sequence over a reverse-Telnet connection, and responds to a resulting prompt immediately, before the BREAK has finished. This problem does not occur prior to Cisco IOS Release 11.3(6.5) or Release 12.0(1.4). There is no workaround.

- CSCdm18905

  Cisco Express Forwarding (CEF) drops directed broadcasts in some environments. There is no workaround.

- CSCdm19275

  If you use the Channel Port Adapter (CPA) in a Cisco 7200 series router that runs Cisco IOS Release 11.3(3)T and greater, with CPA microcode 26.0 and greater, the CPA reloads with the following error message displayed in the system log:

  ```
  %XCPA-3-OUTHUNG: Channel2/0 - output stuck - resetting %ECPA-2-MSG: slot2 %XCPA-2-MBX:
  Force dump requested -0
  ```

  There is no workaround.

- CSCdm19926

  If mismatched access control lists (ACLs) are used in encryption maps (for example, one side of the encryption connection has an ACL statement that the other side lacks), existing encryption connections can stop working after some time. There is no workaround.

- CSCdm20762

  CiscoView does not correctly view the down stream channels of a Cisco AS5800 access server because the access server does not show the correct indexes for the CAS group. There is no workaround.

- CSCdm21388

  SNMP get-next requests might loop on MAC accounting in Cisco IOS Release 12.0(3.6)S.

  Workaround: Create a view that excludes this portion of the tree “ciscoIpStatMIB.1.2.1.”

- CSCdm23824

  Using any form of RSP turbo switching (optimum/flow/CEF), on any type of Ethernet interface (10 Mb/100 Mb/Gigabit), can cause packet errors in the MAC address fields of packets that are input from any interface sharing the same MEMD packet free pools as the Ethernet interface.

  Workaround: Disable all forms of RSP turbo switching by configuring **ip route-cache** on all interfaces, or disable MEMD caching by using either the **test rsp cache memd uncached** EXEC command or the **memory cache-policy io uncached** configuration command.

- CSCdm24099

  An array overflow error in the PA-A3 periodic management code might cause memory corruption on Cisco 7200 series routers. Cisco 7500 series routers do not experience this problem. There is no workaround.

- CSCdm24281

  A Cisco router with Director Response Protocol (DRP) configured might reload with a “spurious memory access” error. There is no workaround.

- CSCdm24526

  A Cisco 6400 node route processor (NRP) will reload when you turn on Interim Local Management Interface (ILMI) and VC discovery if the Network Service Provider (NSP) configuration includes the **no atm address-registration** command.

  Workaround: Remove **no atm address-registration** from the NSP configuration.

- CSCdm25058

  When the following message is displayed, a temporary condition exists where the buffers are completely used and cannot process another event until a buffer is available:

  ```
  %CSM-1-CAS_MSG_DEPLETED: An error was encountered in enqueuing a CAS message - Msg
  headers not available.
  ```

  There is no workaround.

- CSCdm25601

  H.323 inspection in Context-based Access Control (CBAC) might cause a Cisco router to reload. There is no workaround.

- CSCdm26108

  You might be unable to ping your own TR-ISL interface with **multiring** configured on a Cisco 7507 router if it is connected to a Catalyst 3900 Series Token Ring switch. There is no workaround.

- CSCdm27917

  The **ds0 busyout** command does not survive on a Cisco AS5800 access server if any of the following occur:

  – The access server is reloaded

  – The DS3 cable is pulled or replaced

  – You issue the **shutdown** command followed by the **no shutdown** command on the T1 controller

  – The **clear controller t1** command is used

  There is no workaround.

- CSCdm29693

  The “cmCallDuration” variable returns wrong values for timeticks. When compared with system up-time, this variable increases 10 times faster for a call that is in progress during a period of 50 timeticks. There is no workaround.

- CSCdm30609

  Cisco routers that originate a L2F or L2TP packet over an ISL interface might reload.

  Workaround: Turn off fast switching.

- CSCdm30788

  Catalyst 5000 RSM modules that experience spurious error interrupts might cause a C5IP to take a fatal error. The symptoms of this condition are a C5IP error message indicating no status in the cause register and an exception dump. The RSM will recover the C5IP automatically within 30 seconds. There is no workaround.

- CSCdm31643

  A Cisco 3620 or Cisco 3640 router running Cisco IOS Release 12.0(3) or Release 12.0(4) with NM-1ATM-25 will output corrupt packets when the router is transmitting packets of various sizes over an ATM PVC. When received at the other end of the PVC, the packets will generate cyclic redundancy checks (CRC) errors for every packet received. The packet sizes that fail are multiples of 48 bytes (ATM cell payload). All pings fail between the Cisco 3620 and other ATM attached devices if either side initiates an extended ping with a size of 128, 176, or 204 bytes. For every ping, a CRC error is seen on the ATM interface of the receiving device. When the router is pinged from a SUN workstation with 100-, 148-, or 196-byte pings, all pings will fail. Pinging to and from the router with any other ping packet size is successful. There is no workaround.

- CSCdm31647

  If you reset a VIP card in slot 8 of a Cisco 7513 router, the VIP might reload. When the VIP comes up, the ISL trunking to slot 4 (PA-2FEISL-TX) might drop large packets. Small packets go through the interface properly.

  Workaround: Reload the router.

- CSCdm31778

  After a Cisco router reloads, or after CEF is enabled, the router might receive entries for the interface IP address that are not in the CEF table. The CEF interface might be marked as “down” even though the interface is “up.” This causes packets that are destined to the router to be dropped, or transit packets to be dropped due to incomplete adjacency. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdk44289

  On rare occasions, a network can be active in the RIP table and be displayed in the **show ipx route** display, but be unreachable. This condition occurs when most routes are learned through a specific interface or neighbor that goes down long enough to occupy the majority of the route reach hold-down time (4 minutes). If the neighbor or route comes back before the route is removed from the table, there is a chance that some of the routes might be active but unreachable. A symptom of this is a “uses” counter of zero on the output of the **show ipx route detailed** command, even though

devices are trying to reach this network. If services are associated with this network, they time out of the service table, and SAP entries received for these services are rejected due to the "no network found" as seen with **debug ipx sap event**.

Workaround: Clear the specific route entry using the **clear ipx route** {*network*[*network-mask*]|**default**|*} command, or clear the entire route table using **clear ipx route**.

- CSCdk44520

  IPX EIGRP will not see its neighbor when running over virtual templates. If you configure an IPX numbered interface and **ipx ppp-client lo x**, IPXCP comes up but not the IPX EIGRP adjacency.

  Workaround: Use the **interface multilink** command, which is in Cisco IOS Release 12.0 T.

- CSCdm12190

  In redundantly connected networks that run IPX-EIGRP, some obsolete IPX services might not age out and cause a "SAP loop" when **ipx maximum-paths** is set to a value greater than one. This is seen primarily with network connected IPX printers whose SAP service hopcount is one more than that of the route (network) to the service.

  Workaround: Temporarily "down" the network to the service. Also, set **ipx maximum-paths** to one, which is the default to prevent future recurrences. Another potential workaround is to issue the **ipx server-split-horizon-on-server-paths** command. By default, split horizon blocks a router from advertising periodic SAP information to the interface on which the best route to that SAP is learned. But in the case where the SAP might be learned from interfaces other than (or in addition to) the interface on which the best route to that SAP is learned, enabling **ipx server-split-horizon-on-server-paths** will reduce unnecessary periodic SAP updates. SAP will not be advertised to the interface from which it was learned. This will also prevent a potential "SAP loop" in the network.

- CSCdm21357

  Under certain conditions, IPX-EIGRP is leaking memory by way of "IPX USV" and "IPX SAP PH." The condition is likely to occur when there are slow or congested WAN links with a large number of IPX services (SAPs) being advertised, and where IPX-EIGRP neighbors are flapping. This is evident by the constant short "Uptime" and constant non-zero "Q Cnt" from the **show ipx eigrp neighbors** command.

  Workaround: Increase the interface bandwidth with the bandwidth *n* command, or increase the EIGRP bandwidth for that interface with the ipx bandwidth-percent eigrp *as-number percent* command. By default, EIGRP gets the maximum of 50 percent of the interface bandwidth.

Protocol Translation

- CSCdk67438

  When you run Cisco IOS Release 11.3, and use TCP to X.25 PVC protocol translation, it is possible that the PVC will close too quickly. This could potentially cause the PVC to be taken down prematurely causing some data to be lost. When you print over TCP to X.25 PVC protocol, the translation might experience a loss of the last data blocks. There is no workaround.

TCP/IP Host-Mode Services

- CSCdm07904

  Configuring an X.25 tunneling over TCP (XOT) session over an ISDN is problematic when the XOT sessions are closing. The ISDN session might hang up and come back up (on and off) periodically until the underlying TCP session gets completely closed. Usually, the TCP sessions should close, but due to a caveat in TCP for "simultaneous close," the ISDN does not hang up until a timeout of 8 minutes is reached. Users notice a delay of approximately 8 minutes in ISDN hangups.

  Workaround: Use the **show tcp brief** command to list all the TCP connections, and kill the TCP connection (using the **clear tcp tcb** *tcb address* command) that has had the "FINWAIT1" state on it for a long time.

- CSCdm13759

  If the number of User Datagram Protocol (UDP) echo requests from different source/port pairs causes a Cisco router to activate more than a certain number of UDP echo daemons, the remaining UDP echos will not be replied to. There is no workaround.

- CSCdm15751

  If remote copy protocol (rcp) is configured on Cisco routers, and it is used on hosts and routers seperated by a firewall with strict access controls lists (such as allowing only loopback addresses), the rcp sessions fail when multiple interfaces are used on the router and a second interface (other than the primary interface) is configured for rcp sessions using the **ip rcmd source-interface** command.

  Workaround: Use the same IP address for second TCP connection as was use for the first, regardless of what is set in the **ip rcmd source-interface** command.

Wide-Area Networking

- CSCdj80855

  Under some circumstances, X.25 tuneling over TCP (XOT) service might cause a Cisco router to reload. This condition occurs if the record of an XOT host is freed (for example, if all active connections to that host are terminated) while an operation is executed that works with all XOT remote host records (for example, **show x25 xot**). The most common way to evoke this problem is to use the **show** command to report on XOT VCs from a terminal that suspends the reports with the "-more-" prompt.

  Workaround: Configure the terminal not to suspend output. For example, issue the **terminal length 0** command.

- CSCdk19791

  X.25 to TCP protocol translation stops sending X.25 layer-3 "acks" when using PVCs. There is no workaround.

- CSCdk43181

  A Cisco AS5800 access server running Cisco IOS Release 11.3(5)AA cannot accept ISDN calls, but asynchronous calls are accepted.

  Workaround: Dial in with a 56-kbps linespeed.

- CSCdk68801

  The default input size for ISDN D channels might become set to zero. There no workaround.

- CSCdk70598

  When using Point-to-Point Protocol over Asynchronous Transfer Mode (PPP over ATM), or over Frame Relay (PPP over Frame Relay), enabling timeouts on the virtual template will cause the Network Control Protocol (NCP) layer to drop after the timeout. The Link Control Protocol (LCP) will remain open. No network layer traffic will be able to pass across this link.

  Workaround: Manually clear the PPP session from the remote equipment, or issue the **shutdown** command followed by the **no shutdown** command on the ATM or Frame Relay interface (or subinterface) on the gateway router. This will terminate the PPP over ATM or the PPP over Frame Relay.

- CSCdk70741

  For Cisco IOS Release 11.3, it is recommended that you do not run PPP Reliable Link with Link Quality Monitor (LQM). Running it might cause the line to flap with even moderate values of quality (for example, 70). There is no workaround.

- CSCdk76245

  Cisco access servers that have been configured for AODI/X.25/BAP/MPPP with the **ppp multilink idle-link** command will cause problem for non-AODI clients that are using MPPP. The MPPP client that is connected with more then one B-channel will have the first channel in "receive" mode and the rest belonging to the same bundle in normal mode (send and receive). There is no workaround.

- CSCdk78238

  A Cisco router that is configured with **callback-secure** and **callback-accept** should disconnect all incoming calls. However, if a Microsoft Windows Dialup Networking client calls and authentication is passed, the call can stay up. There is no workaround.

- CSCdk82155

  When an LLC session is established on a serial interface, TEST frame stops responding for other LLC sessions. There is no workaround.

- CSCdk90789

  A Cisco router might reload because of an erroneous pointer at fr_bq_proc() function. This condition occurs with routers that run Cisco IOS Release 11.2 P (or later releases) with Frame Relay broadcast queuing in use under heavy multicast traffic. This problem is only seen when using RSP software.

  Workaround: When running Cisco IOS Release 11.3 or later, disable the Fame Relay broadcast queue by issuing the **no frame-relay broadcast-queue** interface-level configuration command.

- CSCdm00844

  A PPP peer might be able to request an IP address that belongs to an address pool other than those they are authorized to use. There is no workaround.

- CSCdm01061

  A Cisco Layer 2 Tunneling Protocol network server might reload when bundling Multilink members that originate from two Layer 2 Tunneling Protocol network servers. There is no workaround.

- CSCdm01992

  When LECS mastership changes from Fast SSRP aware LECS to old-style LECS, and the LES changes from old-style to new-style LES, all clients should join to the new-style primary LES. However, in some situations the new-style clients (Fast SSRP aware clients) stay joined to the secondary LES (old style LES) instead of joining to the primary LES (new style LES). This problem occurs in Cisco IOS Release 11.3 and Release 12.0.

  Workaround: Upgrade to Release 11.2(12) if you are running Release 11.2 images. Upgrade to 11.3(8)WA(4.11) if you are running Release 11.3 images. Upgrade to Release 12.0(4.1) if you are running Release 12.0 images. These upgrades will only give you guaranteed backward compatibility. To get the full benefits of Fast SSRP, all images should be upgraded to at least Release 12.0(5)T.

- CSCdm04447

  The Frame Relay route statement is deleted from the configuration when DLCI is removed due to a leased-line disconnection. There is no workaround.

- CSCdm06362

  A Cisco router might not react to a frame sent by a Vax if the frame is an LLC2 frame (DISC) with the P bit set. There is no workaround.

- CSCdm12648

  All platforms running MLP might potentially encounter a transient error condition where no links are assigned to a multilink bundle. There is no workaround.

- CSCdm14618

  With load sharing multiple HomeGateways from one network access server (NAS) in a VPDN configuration, the NAS only uses the IP address to determine the tunnel ID to be used. This condition occurs even if a different tunnel ID is returned by way of RADIUS.

  Workaround: Have your RADIUS or configuration only return one home gateway to the NAS for use.

- CSCdm18137

  A Cisco 7206 ISDN router that runs Cisco IOS Release 11.3(8)AA1 might experience unexpected PPP LCP timeouts. An error message similar to the following is displayed:

  ```
  Mar 10 05:54:03.774: Se1/0:12 LCP: State is Listen Mar 10 05:54:03.850: Se1/0:12 PPP:
  I pkt type 0xC021, datagramsize 21 Mar 10 05:54:03.850: Se1/0:12 LCP: I CONFREQ [Listen]
  id 0 len 17 Mar 10 05:54:03.850: Se1/0:12 LCP: MagicNumber 0x0000022C (0x05060000022C)
  Mar 10 05:54:03.850: Se1/0:12 LCP: PFC (0x0702) Mar 10 05:54:03.850: Se1/0:12 LCP: ACFC
  (0x0802) Mar 10 05:54:03.850: Se1/0:12 LCP: Callback 6 (0x0D0306) Mar 10 05:54:05.774:
  Se1/0:12 LCP: TIMEout: State Listen Mar 10 05:54:05.774: Se1/0:12 LCP: O CONFREQ
  [Listen] id 2 len 15 Mar 10 05:54:05.774: Se1/0:12 LCP: AuthProto CHAP (0x0305C22305)
  ```

  There is no workaround.

- CSCdm19188

  An ISDN interface might loose packets and headers when the switch type is PRI_4ESS or PRI_5ESS, a connect request is sent by the router, and the switch dose not respond to a connect within T313. This causes the connect to be retransmitted, and the packet and header memory to not be released. There is no workaround.

- CSCdm19619

  PPP is put into an “AUTHENTICATING” phase if virtual private dialup network (VPDN) authorization fails. This condition did not exist prior to Cisco IOS Release 12.0(3)T when VPDN is entered only if PPP is in “AUTHENTICATING” phase.

  Workaround: Restore the PPP phase after the VPDN authorization failure.

- CSCdm22162

  STAC compression LZS DCP gets stuck in an “R-Req” loop. This problem occurs with Cisco IOS Release 11.1 or Release 11.2 hardware compression with an RSP on one end of a connection and Release 11.3 or Release 12.0 software compression on the other.

  Workaround: Disable compression if you are using a Cisco 7500 series router. If you are using a router without an RSP, use software instead of hardware compression on both sides of the connection, or disable compression.

- CSCdm26875

  Deconfiguring an ISDN interface can result in a bus error or spurious access. There is no workaround.

- CSCdm31907

  A LANE subinterface that is shut down might be reported as “Active” from an HSRP perspective. There is no workaround.

- CSCdm32526

  A Cisco router might not be able to pass traffic while using HDLC encapsulation or if STAC compression is enabled. This problem is caused by board encapsulation when setting the compression notification bit in the HDLC header. This is only a problem with high-end routers.

  Workaround: Disable compression.

- CSCdm33448

  If you have a Telematics router connected to one serial interface of a Cisco 7513 router running Cisco IOS Release 12.0(4.0.2)T1, with a second Cisco 7513 router running Release 11.2 connected to the first router’s other serial interface by way of an X.25 hunt-group, the Cisco 7513 router running Release 12.0(4.0.2)T1 will act as an X.25 switch. If the Cisco 7513 router running Release 11.2 is reloaded, the Cisco 7513 router running Cisco IOS Release 12.0(4.0.2)T1 will also reload. There is no workaround.

- CSCdm38212

  Outgoing calls fail on Cisco routers with PRI interfaces when the switch is NI2. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(4)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(4). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdk11064

  If DTR is low on a line to which a Microcom modem is attached (for example, because **modem dtr-active** is configured on the line), CSM nonetheless routes the call to the modem. The result, given the default Microcom modem configuration of "&D," is a "ring-no-answer." Compare the behavior with MICA modems (if DTR is low), then CSM refrains from routing the call to the modem. The result is that if no modems are available and have high DTR, the caller wins a busy. This means that there is no general way to configure Microcom modems for dial-out only. (If the NAS is connected to the network through ISDN rather than CAS, then you can configure DNIS modem pooling and put the dial-out-only modems into a pool with an unused DNIS number. However, this technique does not work for CAS, because DNIS modem pooling is not supported for Microcom modems.)

  Workaround: Use MICA modems instead of Microcom modems.

- CSCdk72998

  The following changes have been made to the rs_async_clearoutput() function to prevent the router shelf from reloading under high load conditions:

  – The call to crashdump(0) has been removed.

  – Instead of calling crashdump(0), only a warning message is issued for the case that should not happen. The router shelf should never reload when there is a failure to allocate a particle buffer.

  – The particle buffer allocation strategy has also been changed so that instead of returning all particle buffers and then trying to allocate a new one, not all the particle buffers are returned. If there were (n) particle buffers, only (n-1) are returned. By keeping the last one, it avoids a call to rs_async_get_particle(), which could fail to allocate a new particle buffer.

- CSCdk80119

  A Cisco AS5200 access server that is configured for **pri-group** can hang during boot (and only during boot) if one or both of the T1 and E1 interfaces receives excessive "short frame" errors (also known as runts) from the lines. This problem might occur where there is an unprovisioned PRI line, or an incorrectly provisioned PRI line.

  Workaround: Disconnect the faulty T1 or E1 line, or configure **loopback** on the affected T1 or E1 controller.

- CSCdm00811

  Malloc failures might be seen on a Cisco AS5300 access server when virtual templates are configured under heavy stress conditions.

  Workaround: Configure the input hold queue size on virtual template to 10.

Basic System Services

- CSCdj84652

  The maximum transmission unit (MTU) size of interfaces that use the encryption service adapter (ESA) is 16 Kbytes.

  Workaround: Configure the MTU to be no larger than 16K (16384) bytes on all interfaces that use ESA.

- CSCdk28278

  Currently generic traffic shaping and Frame Relay traffic shaping are not supported with turbo (optimum/Cisco Express Forwarding [CEF]) switching modes.

  Workaround: Disable these turbo switching modes to make traffic shaping work over the interface. This workaround allows turbo switching modes to coexist with traffic shaping.

- CSCdk48207

  A Cisco 1601 router that is configured to do async MPPP dial-in might reload. This is an indication of memory corruption. The condition occurs when running Cisco IOS Release 11.2(15a)P. Router, DRAM, and Flash memory replacements did not prevent the router from reloading. There is no workaround.

- CSCdk58782

  A Cisco 7200 series router that is connected to a Catalyst 5000 series switch sends a CDP packet on TrBRF VLAN with the Bridge Protocol Data Unit (BPDU) bit set when the subinterface is shut down. This situation can cause a loop if the Catalyst 5000 series switch is connected to other switches. (See caveat CSCdk57646.) There is no workaround.

- CSCdk66827

  When a Cisco MC3810 multiservice access concentrator is configured for CCS cross-connect, calls might not get connected after a period of time. There is no workaround.

- CSCdk66863

  A Cisco router might reload in “net_periodic.” There is no workaround.

- CSCdk81949

  The entire cpmDS0UsageTable (mib oid .1.3.6.1.4.1.9.10.19.1.1.1.1.5) is not being populated correctly when the following configuration is used:

  ```
  Controller T1 0 clock source line primary cas-group 0 timeslots 1-24 type
  fxs-groud-start
  Controller T1 1 clock source line secondary cas-group 0 timeslots 1-24 type
  fxs-groud-start
  ```

  Among the 24 channels, only entries for the first channel of each of the two DS-1s are populated. There is no workaround.

- CSCdk84420

  The **write core** command does not dump the I/O memory on Cisco 3600 series routers. There is no workaround.

- CSCdk93279

  A Cisco AS5800 access server with TACACS+ might restart with the following error:

  ```
  System was restarted by bus error at PC 0x60446D10, address 0x1C
  ```

  This occurs when the Cisco AS5800 is near T3 capacity, with users dialed in, and when the TACACS+ server that the access server is pointing to has to be changed. There is no workaround.

- CSCdk93315

  Any image which does not include the Layer 2 Forwarding Protocol (L2F) subsystem will reload when an L2F packet is received. When the system reloads, no crash information is obtained, and the fault history (obtained by issuing **show context**) is also often out of date.

  Workaround: Check for misconfigured tunnels on the network that might be sending L2F packets to the router.

- CSCdm01018

  If you issue the show buffers command on a Ciscos MC3810 multiservice access concentrator, the FRF Seg Pool buffers might report numerous “misses.”

  Workaround: Move the FRF Seg pool to private pool.

- CSCdm02704

  Accounting stop records for connection service should be generated before aaa user_struct is freed. Appropriate pointer checking is also needed for preventing memory access violation. There is no workaround.

- CSCdm07937

  If you repeatedly executed the **write terminal** command on a Cisco 12000 Series Gigabit Switch Router (GSR), the GSR might shut down due to environmental alarms. The env table that is used to compare measured readings is being corrupted. There is no workaround.

IBM Connectivity

- CSCdk61220

  A Token Ring LANE client might not come up immediately when configured on a Cisco 4500 ATM interface. There is no workaround.

- CSCdk72916

  Lexmark printers are contacted by a central server that is sending single route explorer to the following MAC address: FFFF.FFFF.FFFF. In Cisco IOS Release 11.1, using RSRB without local-ack, this explorer is passed to the remote Token Ring. With Cisco IOS Release 11.2 and Release 11.3 this no longer happens.

- CSCdk78156

  If you remove **source-bridge ring-group** *xxx*, and *xxx* is not being used under any interface, the LLC2 session is dropped. There is no workaround.

- CSCdk83457

  While doing RSRB local-ack with priority peers, the following error message might appear:

  ```
  %TCP-2-INVALIDTCPENCAPS:Invalid TCB encaps pointer :
  ```

  Workaround: Turn off priority peers or turn off local-ack.

- CSCdk84269

  Token Ring LAN Emulation Client (TR-LEC) currently processes all registration requests received on its control distributed virtual circuit. It should only be doing this if the LANE client identifier (LECID) in the registration message matches up with its own LECID. The LEC finite state machine (FSM) invokes a_resend_reg_req when a negative reg_rsp is received. Instead, you should invoke a_process_reg_rsp. There is no workaround.

- CSCdk86081

  The downstream physical unit (DSPU) does not allow any new DSPU connections, and the following messages appear in the router log:

  ```
  %DSPU-3-LSConnInFailedNoMem: Connect in from remote address 00104b0a60e0 failed ;
  insufficient memory %DSPU-3-LSConnInFailedNoMem: Connect in from remote address
  00105a00e326 failed ; insufficient memory
  ```

  There is no workaround.

- CSCdk89189

  A Cisco 2600 series router that runs DLSw with priority and backup peers over BRI might reload with SegV exception.

  Workaround: Do not have priority peer configuration.

- CSCdk90257

  A second link fails to reactivate during recovery. Both links must be restarted in sequence so the links will activate the first link as transmission group 21 (TG21) and second link as TG22. Otherwise, the failing link stays in TG0 state, attempting to reconnect.

  Workaround: Assign specific TG numbers (from 1 to 20) to parallel TGs.

- CSCdk93916

  An Advanced Peer-to-Peer Networking (APPN) router might reload with the following backtrace message:

  ```
  0xRA:0x60757578:Qdeq(0x6075756c)+0xc 0xRA:0x606FBA6C:hs_deleter(0x606fb930)+0x13c
  0xRA:0x606FC038:mu_processor(0x606fbe40)+0x1f8
  0xRA:0x606FC77C:remote_path_control(0x606fc650)+0x12c
  0xRA:0x606FDC04:pc_mainline(0x606fd500)+0x704
  0xRA:0x606F8D70:xxxpcasm(0x606f89d0)+0x3a0
  ```

  There is no workaround.

- CSCdm00997

  APPN Berkeley Internet Name Domains (BINDs) from low entry networking (LEN) nodes, such as MS SNA-Server, might fail in a pending active state when the router is also an intermediate node. The BIND transmission header (TH) is corrupt in the forwarded direction, which is then typically dropped by the receiving device. There is no workaround.

- CSCdm02196

  A Cisco 7206 router might reload with a bus error with the following message:

  ```
  System restarted by bus error at PC 0x6087AD40, address 0x244
  ```

  This only happens directly after the router is reloaded. After the router is up and running the system is stable. There is no workaround.

- CSCdm05337

  An APPN router might reload with the following stacktrace:

  ```
  RA: 0x601C89D4[abort(0x601c89cc)+0x8] RA: 0x601C7354[crashdump(0x601c728c)+0xc8] RA:
  0x607375F0[Eattach(0x60737588)+0x68] RA: 0x60739DCC[Pcreate(0x60739cd4)+0xf8] RA:
  0x60648720[amp610(0x606486c0)+0x60] RA: 0x6064789C[amp500(0x60647510)+0x38c] RA:
  0x60645AD0[amp00(0x60645790)+0x340]
  ```

  In this situation, the router uses excessive processor memory when multiple ENs (over 100) register resources to this NN at the same time. There is no workaround.

- CSCdm05685

  A Cisco router might reload if DLSw priority peers and Downstream Physical Unit (DSPU) over virtual data-link control (VDLC) are configured together. This condition also occurs when DLSw priority peers and Systems Network Architecture (SNA) over VDLC are configured together.

  Workaround: Use regular DLSw peers.

Interfaces and Bridging

- CSCdj54192

  An interface on a HSSI 1 port adapter (PA-H or H1T+) might go down/down and display the following error message (XXXX represents the affected interface):

  ```
  %MUSELIX-1-STOPFAIL: XXXX: Stop Failed at disable port
  %MUSELIX-1-STARTFAIL: XXXX: Start Failed at enable port MUESLIX-1-FAILURE_CAUSE:
  SerialX/X:
  ```

  Issuing the **shutdown** and **no shutdown** commands has no effect. There is no workaround.

- CSCdk33589

  A router might reload when traffic shaping is configured on an ATM interface. There is no workaround.

- CSCdk47517

  When a four-Port Token Ring 4/16-Mbps port adapter (PA-4R) is used on a congested or unclean Token Ring, the VIP port adapter might exhibit the following errors and traceback:

  ```
  > Sep 17 14:04:26 EDT: %IPC-5-SLAVELOG: VIP-SLOT4: > IBM2692-1-SRBQ_OVERFLOW: IBM2692
  (0/0), SRB queue overflow. > Sep 17 14:11:03 EDT: %LINK-3-UPDOWN: Interface
  TokenRing4/0/0, > changed state to > up EDT: %IPC-5-SLAVELOG: VIP-SLOT4: > > Sep 17
  14:12:22 SYS-2-GETBUF : Bad getbuffer, bytes= 50765 > Sep 17 14:12:21 EDT:
  %IPC-5-SLAVELOG: VIP-SLOT4 : > Process= “<interrupt level>”, ipl= 1 > Sep 17 14:12:21
  EDT: %IPC-5-SLAVELOG : VIP-SLOT4: > Traceback= 6005DFAC 600D18B4 600D1CEC 600D215C
  600D28EC
  ```

  There is no workaround.

- CSCdk52565

  If you use a Cisco 7500 series router, a CT1/CE1 port adapter, PPP distributed hardware or software compression, and Cisco IOS Release 11.2 P or below in conjunction with a remote router running PPP software compression and Cisco IOS Release 11.3 or greater, a reload in LZS_Decompress, or an “output stuck” error message might occur on the Cisco 7500 series router.

  Workaround: Run Cisco IOS Release 11.2 P (or below), or Cisco IOS Release 12.0 (or above), on both routers.

- CSCdk69514

  The Ethernet interface of a Cisco 2600 series router that runs Cisco IOS Release 12.0 might not come back up when the interface is flapping.

  Workaround: Issue the **clear int** command.

- CSCdk77411

  Although a Bridge-Group Virtual Interface (BVI) can receive Internetwork Packet Exchange (IPX) packets, BVI cannot send IPX packets. There is no workaround.

- CSCdk79774

  Under heavy load conditions, a Cisco 7000 family router with VIP-based PA-4R, PA-4R-FDX, or PA-4R-DTR Token Ring interfaces may forward packets containing four extra bytes. The four bytes are appended to the end of the packet. This might adversely affect protocols that are sensitive to frame lengths (for example, IBM SNA sessions may fail). There is no workaround.

- CSCdk80140

  When Multilink is configured over a serial interface, long delays occur with large packets. The problem is only seen when fair-queueing is configured on the interface.

  Workaround: Disable fair-queing.

- CSCdk80653

  Frames that are 33 bytes or less are being corrupted when bridged between a FDDI interface and a PA-A1 in Cisco IOS Release 11.1(19)CC1 or above. The following are workarounds for this problem:

  – Replace the PA-A1 with a PA-A3.

  – Replace the FDDI interface with another interface type, for example, Token Ring or Ethernet.

  – Downgrade the router to Cisco IOS Release 11.1(18)CC or below.

  – Disable fast switching for transparent bridging.

- CSCdk85960

  When ATM subinterfaces belong to a bridge group, and the bridge group is part of a BVI, multicast packets are not forwarded. There is no workaround.

- CSCdk89313

  Currently, there is no NetFlow support for BVI interfaces or any interfaces in a bridge group. There is no workaround.

- CSCdm08904

  The **show controllers t3** command on CT3IP did not provide the correct hardware version information. This is only a display problem. There is no impact on functionality. There is no workaround.

IP Routing Protocols

- CSCdi84140

  IP access lists always permit IP fragments. There is no workaround.

- CSCdk27181

  Cisco IOS Network Address Translation (NAT) socket translation only works for connections initiated from outside to inside. Without sockets, translation works on the IP address. With socket translation, it does not. The version is c1605-nosy-mz.112-14_P. There is no workaround.

- CSCdk40576

  A Cisco router might reload after an upgrade to Cisco IOS Release 11.2(15). There is no workaround.

- CSCdk64629

  NAT only translates the first address entry in a NetBIOS Name Service (NBNS) group name response message. Other group name address entries are not translated, and therefore the NetBIOS client is only able to reach the first group address host. This happens because the client would be using an inside local address from the outside for the other members of the NBNS group name. There is no workaround.

- CSCdk74808

  When IP unicast RPF check is enabled on one subinterface, all the subinterfaces on that interface have the check performed. This includes subinterfaces that were deleted. This situation might cause the router to drop packets that do not pass the reverse-path test. Note that this might only be an issue for asymmetric routes.

  Workaround: Disable the IP unicast RPF check on the subinterface that has it enabled. If this subinterface has already been deleted, it must be configured again and the RPF check must be disabled. The subinterface might be deleted again after this is done.

- CSCdk78845

  When the prune-timers in the oil list are not identical, the mroute will still go to a “forwarding” status even when there is no listener. There is no workaround.

- CSCdk81888

  OSPF might reload if a corrupt protocol packet is received and the corruption is not detected by the IP checksum. Because the IP checksum detects most packet corruptions, a reload is highly unlikely unless a large percentage of OSPF packets are corrupt.

  Workaround: Fix the source of the packet corruption, or shut down the link on which the incoming packets are received.

- CSCdk82872

  After a file with a large filename is transferred, Cisco IOS Network Address Translation (NAT) does not translate the embedded IP address in the **ftp port** command.

  Workaround: Close the FTP session and open a new one.

- CSCdk87469

  OSPF External type-1 routes that are added to the routing table are not removed once that route is gone. This is seen in Cisco 7000 series routers running Cisco IOS Release 12.0(2)S as well as Cisco AS5200 access servers running Cisco IOS Release 12.0(2)T.

  Workaround: Clear the routing table or redistribute external routes as type-2.

- CSCdk83829

  If the physical memory of a system is completely exhausted with huge number of routes and peers, a Cisco router might reload. There is no workaround.

- CSCdm05440

  Selective Packet Discard (SPD) can erroneously discard “hello” packets from some routing protocols, such as OSPF, EIGRP, and HSRP. When a router is processing many other packets at process level, the lost routing protocol packets can cause route and HSRP “flapping,” leading to intermittent data packet loss. There is no workaround.

ISO CLNS

- CSCdk00465

  If you convert from DECnet phase IV to DECnet phase V with multiple paths, you might experience routing loops.

  Workaround: Configure equal metrics for all paths.

Miscellaneous

- CSCdj22429

  Under rare circumstances, the Cisco AS5200 access server might issue the following message:

  ```
  %SYS-3-BADMAGIC: Corrupt block at 20000000 (magic xxxxxxxx)
  ```

  The Cisco AS5200 crashes with a software forced error. There is no workaround.

- CSCdk32594

  Initializing a BRI that is connected to a Siemens HICOM PABX fails, leaving the Layer 1 Status in ACTIVE_ErrorInd.

  Workaround: Disable Cisco Discovery Protocol (CDP) on the interface.

- CSCdk58181

  Packets are decrypted when received from an input interface, and then encrypted again before being forwarded to the output interface. There is no workaround.

- CSCdk60886

  After you place a fax call to the Public Switched Telephone Network (PSTN) from a remote Foreign Exchange Office interface (FXO) port using connection trunk, the call never disconnects properly. You must issue the **shut** command followed by the **no shut** command to bring the port back into operation.

  Workaround: Use the private line auto ringdown (PLAR) connection, or nothing at all.

- CSCdk65092

  When you use the RSP platform with ESA installed, crypto sessions might stop encrypting data, but the access lists continue to see matches. A **show crypto engine connections** *slot* command shows the interface as "???" instead of the physical interface through which the packets should be going. The symptom is that although the crypto session appears to be up according to the **sh crypto conn** command, you are unable to send any data to the other side if it is to be encrypted according to the crypto map.

  Workaround: Remove the crypto map from the interface and then remove the corresponding sequence number from the crypto map. Re-create the sequence into the map (using the same configuration commands) and apply it back to the interface.

- CSCdk65594

  In certain configurations, CEF drops every other outgoing packet on an ATM interface. The problem occurs with RFC 1577 SVCs, and with RFC 1483 PVCs that use Inverse ARP.

  Workaround: Disable CEF on the affected ATM interface with the **no ip route-cache cef** command.

- CSCdk66567

  If Token Ring is the endpoint of an encrypted tunnel, extra packets are generated. The symptoms of this problem are a high CPU load (mainly taken by the Crypto Engine) and false addresses when enabling the **debug tunnel** command.

  Workaround: Use the **tunnel sequence-datagrams** interface command on both endpoints of the tunnel.

- CSCdk69456

  The data encryption service adapter (ESA) Crypto engine in a VIP2 is limited to 25 connections. New connections are establish after a key exchange, but no encryption and traffic flow take place. This condition occurs in the Cisco 7507 router. There is no workaround.

- CSCdk70139

  Committed Access Rate (CAR) is not working for an input list with the access list checking a MAC address. This is seen on low end platforms (Cisco 2600 series, Cisco 3600 series and Cisco 4500 routers). There is no workaround.

- CSCdk70753

  Robbed bit signalling on a Cisco AS5800 access server fails under certain circumstances. This results in digital signal level 0 (DS0) channels returning busy signals when they are called. The Cisco AS5800 T3 controller sees ABCD bits of 0000 when the Telco has seized the line with ABCD bits of 1100. There is no workaround.

- CSCdk72928

  On a Cisco 7513 router running Cisco IOS Release 11.1(20)CC with **fddi mac-accounting** configured, there is a discrepancy between the CLI output from the **show interface fddi 5/0/0 mac-accounting** command, and the **snmpwalk** output for "cipMacSwitchedPkts." The SNMP data is missing all output entries except those destined for ffff.ffff.ffff. There is no workaround.

- CSCdk76577

  When a router is the origin of many routes that pass through tag-switched path (TSP) tunnels, and dynamic tag-switching is disabled, a watchdog timeout might occur when one of these routes is deleted.

  Workaround: Do not disable dynamic tag-switching, or avoid deleting routes which go through TSP tunnels (that is, traffic engineering or static routes through TSP tunnels).

- CSCdk78652

  The PA-A2 ATM-CES port adapter driver might free twice for aborted TX packets and particles. This might happen when you change shaping parameters or shut down while active traffic is going through the port adapter. There is no workaround.

- CSCdk79219

  On a Cisco 7200 series router, if you change an interface configuration while there is active traffic or reset the interface while there is active traffic, the router might reload. This problem occurs with a PA-A3 hardware revision 2.0 port adapter.

  Workaround: Stop the traffic completely before the operation.

- CSCdk79550

  When a Cisco AS5800 access server is reloaded with the D-channel in a shut condition, issuing a **no shut** command on the D-channel does not bring the PRI back in service. This situation happens on both T1 and T3 feature boards.

  Workaround: Issue a **shut** command followed by a **no shut** command on the corresponding T1 controller to make the PRI operational.

- CSCdk80140

  When multilink is configured over a serial interface, a lengthy delay is observed, typically with large packets. The problem is seen only when fair-queueing is configured on the interface.

  Workaround: Disable fair-queing.

- CSCdk80477

  If you run Cisco IOS Release 12.0(1) with an RSM in a VIP2-40 with a PA-A3 port adapter, the RSM might reload. When this happens, you can recover the RSM by disabling and reenabling the ATM interface. There is no workaround.

- CSCdk81653

  If you issue the **show file** [*device*:] *filename* command on a directory, without specifying the filename, a Cisco router might reload. There is no workaround.

- CSCdk82708

  No tag is created for the default route. Routing is possible, but requires that each packet goes to the CPU (including LS1010). There is no workaround.

- CSCdk84552

  The fix for a previous caveat (CSCdk77654) inadvertently requires that ACLs attached to crypto maps include ICMP, even if ICMP packets are not intended to be encrypted. Note that ICMP is matched when the IP protocol is specified in the ACL. There is no workaround.

- CSCdk84903

  After you reload a Cisco 7500 series router that runs Cisco IOS Release 12.0(2.5)S, the packet over E3/T3 (POET) DS3 interface comes up in a down/down state.

  Workaround: On the DS3 interface, issue the **shutdown** command, then issue the **no shutdown** command. This results in the interface changing to the “up/up” state.

- CSCdk86377

  An interface reset or shut will zero the sustainable cell rate (SCR) of variable bit rate virtual circuit (VBR VC).

  Workaround: Recreate the VBR VC.

- CSCdk86406

  When a virtual terminal line (vty) is used for a non-TCP session, such as for LAT, X.3 PAD or V.120, the router loses approximately 100 bytes of memory for each session. There is no workaround.

- CSCdk86664

  If **ip cef** is turned on, encryption stops working. There is no workaround.

- CSCdk86801

  Conditional debugging called does not trigger debugs when the number is called. There is no workaround.

- CSCdk88225

  An RSP might reload by software forced error when you use one the **no mls rp ip** or **no interface FastEthernet** commands. There is no workaround.

- CSCdk89651

  You might not be able to make two consecutive asynchronous calls from a Cisco AS5300 access server that runs Cisco IOS Release 11.3(7)T. The problem occurs whenever NFAS is configured. The problem goes away when NFAS is removed. With NFAS configured and only one controller up, there is no problem dialing out. There is no workaround.

- CSCdk89833

  After a reload, ATM PVCs disappear from the running configuration.

  Workaround: Configure PVCs after the reload.

- CSCdk89721

  The **show isdn history** command does not show any information. There is no workaround.

- CSCdk90213

  When a Cisco router tries to get a Certificate Revocation List (CRL) from the public key infrastructure (PKI) as part of Internet Key Exchange (IKE) setup, the router reloads. This happens just after the CRL has been requested. There is no workaround.

- CSCdk92381

  TCP/IP traffic that is routed between a TR-ISL subinterface and an Ethernet ISL subinterface might not be fragmented correctly.

  Workaround: Keep the TR-ISL subinterface MTU to 1500, or move the TR-ISL subinterfaces to another hardware interface.

- CSCdk93443

  With distributed CEF, the **clear cef linecard** command can sometime cause CEF to be disabled on some slots.

  Workaround: A microcode reload of the slot will reenable CEF.

- CSCdm00582

  The PA-A3 RX port adapter will stall after a reload.

  Workaround: Issue the **clear interface** command.

- CSCdm03143

  Configuring a Fast Ethernet interface for full duplex does not take the device to full-duplex mode. Also, late collisions are observed. The fix for a previous caveat (CSCdk81069) modified the amdfe driver to logically “or” the existing contents of the PHY control register with the duplex settings. As the autonegotiation enable bit in the control register is set (as the device was autonegotiating before the duplex change), the duplex settings do not take effect. If the device was previously in half duplex, it continues to be in half duplex.

  Workaround: To manually configure speed/duplex on the PHY, autonegotiation needs to be disabled.

- CSCdm05324

  A Cisco router converts a requested TFTP filename request to lower case during an SNMP netConfigSet. If the configuration filename is mixed or uppercase in the tftpboot directory, the file will not be found on a UNIX-based TFTP server.

  Workaround: Use an all-lowercase filename.

- CSCdm06225

  Connectivity problems occur in Virtual Profile situations with a combination of V.120 and native sync-ISDN calls on a Cisco AS5800 access server. A dial-up interface, which last had an incoming V.120 call, can a have problem getting packets across on subsequent calls. This condition occurs if a AAA per-user configuration containing downloaded interface packet filter (access lists) is applied. There is no workaround.

- CSCdm06448

  A PA-A2 port adapter CES part microcode download might fail during bootup. The result is that the port adapter is invisible to the Cisco IOS software.

  Workaround: Reboot the router.

Novell IPX, XNS, and Apollo Domain

- CSCdk81350

  If **ipx down** is configured at the command prompt and **ipx down** is read out of the configuration file at bootup, an IPX route to a directly connected network appears in the routing table. In this situation, new routes to the directly connected network will not be learned, and the network might appear as “down” in the routing table.

  Workaround: Bring up the interface by removing the **ipx down** command, then reissue the **ipx down** command.

- CSCdk86872

  If an interface is administratively down with an IPX network configured, and you proceed to add that network to the IPX EIGRP router, that network (route) gets propagated through EIGRP even though that interface is “down.” The route does not go away.

  Workaround: To remove the network (route) from EIGRP, issue the **no shut** command follow by the **shut** command. Alternatively, remove the network from within the IPX EIGRP router (for example, issue the **ipx router eigrp** *as* and **no network** *net* commands).

- CSCdm00033

  If IPX NLSP RIP OFF is configured and therefore NLSP RIP compatibility mode is off, a reply is not sent to a client who sends a RIP general query, a request for all networks.

  Workaround: Do not to configure IPX NSLP RIP OFF, but leave compatibility mode enabled.

VINES

- CSCdm09771

  A VINES “proxy” memory leak can occur in a router environment where a VINES client application causes a router to act as a proxy server when the client sends service requests directly to a router that it does not support. The router becomes a proxy server when it forwards these same service requests to the nearest Banyan VINES server. The leak can be detected by observing the persistent “Vines Proxy” lines from the output of the **show mem sum** command:

  ```
  0x60433E38 24 2807 67368 Vines Proxy 0x60433E38 28 5246 146888 Vines Proxy
  ```

  There is no workaround.

Wide-Area Networking

- CSCdj71680

  In a DDR environment, a packet that starts a dial might use an incorrect dialer map to reach a remote destination. The problem is intermittent and the same packet might select the proper dialer map upon the next try. There is no workaround.

- CSCdj77057

  Occasionally, the **show dialer map** command causes a Cisco router to reload. This condition only occurs when connections are dropped during the execution of the command. This problem affects Cisco IOS Releases 11.2(11)P and later. There is no workaround.

- CSCdj82342

  Running Frame Relay over ISDN on a Cisco 3640 router initially works, but starts to fail when the interface input queue becomes full and all incoming packets are dropped. The interface input queue wedge problem cannot be resolved by issuing the **lock** or **unlock** commands. The router should be reloaded.

- CSCdk55610

  For Cisco IOS Release 11.2, when you configure more than one dialer string and a dialer load-threshold, additional B-channels will only be opened when they are connected to the first dialer string. When connected to the second dialer string, only one B-channel will be opened, even if the threshold is exceeded. In Cisco IOS Release 11.3, the dialer load-threshold does not work at all. There is no workaround.

- CSCdk61104

  If the group-async interface is part of a dialer interface that does not have PPP authentication turned on, and the **dialer rotary-group** configuration is removed, the PPP users are not authenticated.

  Workaround: Reconfigure either the ppp authentication command or group range command on the group-async interface.

- CSCdk66454

  You might experience a reload using X.25 switching in x25swt_last_resort. There is no workaround.

- CSCdk68549

  Removing the dialer remote-name *name* command might cause a Cisco router to reload if the router is actively trying to dial the named remote site.

  Workaround: Issue the **shutdown** command from config-if mode before issuing the **no dialer** *remote-name* [*name*] command.

- CSCdk72458

  If packets with CCP are compressed when the PAK_PRIORITY bit is set, sequence errors will create compression dictionary resets. This only occurs when there is congestion on the PPP output queue (that is, there are paks waiting there which could be reordered).

  Workaround: In cases of extreme congestion, more bandwidth should be supplied.

- CSCdk73514

  A Cisco AS5200 access server might reload when using Microsoft PPP callback. An error message similar to the following will be displayed:

  ```
  System restarted by bus error at PC 0x22317282, address 0xD0D0D15
  ```

  Workaround: Define static dialer maps.

- CSCdk75078

  If you observe an increase in the number of retransmission requests (REJs) sent out of a router interface, an acknowledgment for a received frame was not sent out. This causes a remote station timer to expire and resend the data. There is no workaround.

- CSCdk75490

  A Cisco AS5300 access server that runs Cisco IOS Release 11.3(7.1)T or later releases might have problems bringing up Layer 2 after ISDN is configured for the first time. This is due to invalid Layer 2 timer values that can been seen in the configuration. The invalid Layer 2 timer values can also be seen when you issue the **show isdn timers** command. Please refer to the following caveats: CSCdk68552 and CSCdk78782.

  Workaround: Save the configuration and reload the router (notice that the error messages because of the invalid timer values are rejected during the processing of the configuration).

- CSCdk76047

  Asynchronous Multilink PPP stops working when a SLIP user gets connected on the asynchronous interface. There is no workaround.

- CSCdk77092

  LAN Emulation (LANE) does not reply to LAN Emulation-Address Resolution Protocol (LE-ARP) requests if the Bridge-Group Virtual Interface (BVI) Media Access Control (MAC) address is different from the ATM's MAC address. As a result, the traffic to the BVI interface gets sent from the LANE broadcast and unknown server (BUS).

  Workaround: Use the same MAC address for both ATM and BVI interfaces.

- CSCdk77947

  A Cisco AS5200 access server running Always On/Dynamic ISDN (AO/DI) in Cisco IOS Release 11.3(6)T1 reloads with unexpected interrupt. There is no workaround.

- CSCdk78063

  L2D_Srq_Task() reads status testing for an active connection. When this fails (as it frequently will the first time) it calls edisms, rechecking status when it returns. It simply retests the status byte, which is now stale. This fix guarantees the validity of the status byte.

- CSCdk80519

  A VIP might reload, followed by an RSP software forced reload. There is no workaround.

- CSCdk80551

  Under heavy usage on an X.25 serial link, a Cisco router running TCP to X.25 translation might reload. There is no workaround.

- CSCdk83115

  A system might be restarted by a bus error at PC 0x602E2090, address 0x11755677. There is no workaround.

- CSCdk84702

  Under certain conditions, PAP authentication request packets are leaked. The leaked packets are not recoverable, and enough memory can be lost that a reload of the router is necessary. There is no workaround.

- CSCdk85274

  When attempting to bring up more than just a few tunnels with Virtual Private Dial-Up Networking (VPDN), CPU utilization rises to nearly 100%. If a single tunnel is used, no performance degradation is noticed. There is no workaround.

- CSCdk86557

  When running PPP in conjunction with NFAS on PRIs the NFAS interfaces that are configured to have 24 B-channels will only be able to negotiate and pass PPP data on the first 23 channels. Calls will be routed to the 24th B-channel but the router is unable to send PPP data out it and thus that user is stuck until PPP times out and they dial in again and get another B-channel.

  Workaround: Take the 24th channel out of service with the **isdn service dsl x b_channel 24 state 2** command.

- CSCdk87834

  On an RSP, L2F Protocol fails to forward fast-switched packets from the tunnel to some physical interfaces (such as PRIs). The L2F neither punts the packets to process nor does it free the packets up. L2F related applications like SGBP and VPDN are affected. There is no workaround.

- CSCdk88413

  When the **random-detect** command is configured, a Cisco router can reload at ISDN call setup. There is no workaround.

- CSCdk92934

  When you enable both Multichassis Multilink PPP commands (**sgbp group** and **sgbp member**) and **vpdn authen-before-forward** on a NAS at the same time, Multilink dial-in users are not able to establish connections.

  Workaround: Turn off **sgbp** or **vpdn authen-before-forward**.

- CSCdk94188

  In certain circumstances, you must set the extend bit in the channel ID when communicating with a Northern Telecom DMS-100 Custom switch. There is no workaround.

- CSCdm00889

  ARAP Callback is negotiated with iMAC dialing in, but is not executed in the Cisco IOS software. There is no workaround.

- CSCdm01059

  Systems can generate bad memory accesses and possibly reload when IPCP completes negotiations on PPP links. This problem was inadvertently introduced with the patches for defect CSCdk13366.

  Workaround: Customers using PPP that have system images into which CSCdk13366 has been incorporated will need to upgrade to use an image that includes CSCdm01059.

- CSCdm01117

  When using the **backup load** command, a software-forced reload might occur when the load threshold is reached. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(3)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(3). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdk66309

  When the **pri** configuration command is issued for a T1/E1 controller, the following message might appear on the console:

  ```
  SYS-3-MGDTIMER
  ```

  There is no workaround.

- CSCdk69102

  A Cisco AS5800 access server that runs Cisco IOS Release 11.3(6.1)AA or a more recent release might experience a system reload following a modem pool download. This only affects the downloading of nondefault firmware and is only experienced a small percentage of the time. This condition might also arise when the access server runs Cisco IOS Release 12.0(1.5) or a more recent release. There is no workaround.

Basic System Services

- CSCdj85843

  VIP cards do not have an accurate sense of time. NetFlow exports, for example, are not synchronized. There is no workaround.

- CSCdk24870

  IP trigger authentication does not work with Multilink Point-to-Point Protocol (MLPPP). IP trigger authentication only works with a single channel. There is no workaround.

- CSCdk38629

  When **voice-encap** is configured on a Frame Relay or Cisco HDLC, all fancy queuing is disabled and only FCFS is allowed.

  Workaround: The new [**no**] **frag-pre-queuing** CLI command has been added to the interface with Frame Relay encapsulation that users can select if queuing is performed after fragmentation. The default setup is **frag-pre-queuing**, which allows only first come first served (FCFS) queuing on the interface level. With the [**no**] **frag-pre-queuing** command, the user can configure weighted fair queuing (WFQ), custom queuing (CQ), or priority queuing (PQ) on the interface level so that all fancy queuing is supported with **voice-encap**. After the [**no**] **frag-pre-queuing** command is issued, the interface queue is not changed. The user needs to explicitly specify WFQ, CQ, or PQ if such fancy queuing is desired. For HDLC encapsulation, fragmentation is moved to after queuing. For HDLC, all fancy queues are allowed with this caveat fix.

- CSCdk46007

  When a Cisco MC3810 multiservice access concentrator that has a large number of Frame Relay PVCs is upgraded to Cisco IOS Release 11.3(1)MA5 or later, the console might display memory allocation failures because of an insufficient big buffer pool of 1680 bytes. There is no workaround.

- CSCdk46621

  When a Cisco router interface is configured as a DCE, it does not track the correct control lead coming from the DTE. The interface stays up and up when the DTR is low. There is no workaround.

- CSCdk50924

  If two users on different tty connections simultaneously attempt to issue commands that access NVRAM (for example, **show startup-config**), the router might reload. There is no workaround.

- CSCdk55631

  After you load a startup configuration by issuing the **copy tftp startup-config** command on a Cisco 3620 router, the NVRAM becomes unreadable on the next reload. During the boot sequence the following messages can be seen:

  ```
  ERROR in NVRAM sizing. NVRAM could be bad! Hardware indicated 32768 bytes. Software
  detected 0 bytes.
  ```

  and

  ```
  %C3600-3-BADNV: Detected invalid NVRAM size: -2056 bytes
  ```

  This condition is extremely rare. To solve this problem, the customer will need to upgrade the ROM Monitor boot ROM with a version that has this fix.

  Workaround: Change each capital V in the configuration to a lower case v.

- CSCdk57202

  When two peer subsystems (EECM-EECM or EECM-TDSM) communicate about a call, they identify the call using their own call instance ID. A race condition occurs after you send a “SETUP” message to the peer if you send a “RELEASE” message (or some other message) before the peer has responded to the “SETUP” message. The peer does not get the call instance ID it expects and therefore the message is lost. There is no workaround.

- CSCdk59099

  AAA connection accounting works for a single connection on the router, but with multiple connections start records are generated for all connections. Only the first disconnected call has a stop record generated; subsequent closed connections do not. All records have the same Acct-session-id. This problem exists in Cisco IOS Release 11.3(2.4)T or later. There is no workaround.

- CSCdk62728

  You cannot enter the **aaa authorization exec tacacs** configuration command. There is no workaround.

- CSCdk63134

  When you boot a Cisco router that has dual Route Switch Processors (RSPs) and multiple VIP interfaces, the slave RSP might not change to the “Running” state, and might remain in the “Halted” state. This condition results from a lack of buffers for IPC communication.

  Workaround: Issue the **slave reload** configuration command once the system comes up.

- CSCdk66856

  SNMP might be unable to get data on Run-from-Flash partitions. There is no workaround.

- CSCdk67339

  When a Cisco 1600 series router is connected in synchronous mode using the “Easy IP” feature, the WIC-1T synchronous/asynchronous might drop the PPP link. This condition is caused by having **ip address negotiated** configured on the serial interface. When a static IP address is configured, the problem does not occur. There is no workaround.

- CSCdk71921

  AAA authentication method lists disappear when you upgrade from Cisco IOS Release 11.2 to Cisco IOS Release 11.3 or later IOS releases. When **aaa authentication local-override** is configured in a Release 11.2 image and AAA authentication method lists have three or more methods defined, upgrading to Cisco IOS Release 11.3 or later IOS releases generates a traceback.

  Workaround: Remove one or more of the methods before the upgrade.

- CSCdk72139

  When Reply-Messages are included in a RADIUS Access-Accept, attributes following the Reply-Message attributes might not be recognized. For instance, if multiple Reply-Messages are included in the Access-Accept, only the first reply message is displayed.

  Workaround: Do not use Reply-Messages in Access-Accept or Access-Reject. If Reply-Messages are absolutely needed in an Access-Accept or Access-Reject, there should be only one attribute and it should be included as the very last attribute in the reply. Reply-Messages in Access-Challenge should work properly.

- CSCdk74502

  No data connectivity can be established across Switch 0 data DLCIs even though a Cisco IGX switch is transmitting normally.

  Workaround: The same DLCI should be used for the end-to-end IP routing data connections (Switch 0 connections). The trunk DLCIs (management, Frame-Relay, and voice DLCIs) should not be used for data or voice connection DLCIs inside of the connect statement.

- CSCdk75174

  The Async-HDLC microcode from Motorola has a problem with certain data transparency (escape) sequences. One known example is the following PPP/LCP sequence sent from a Bay Nautica 4000 router:

  ```
  7e 7d df 7d 23 c0 21 ....
  ```

  It appears that the microcode cannot handle the “7d df” (escaped “0xff”).

  Workaround: Get a new version of microcode from Motorola. Until that happens, another solution is to turn off the Async-HDLC microcode and do not enable “hardware-assisted PPP mode” within the Cisco IOS software. Instead, the Async-PPP framing is done in software (by the Cisco IOS software). To enable this mode of operation, the hidden command [**no**] **microcode-enable** is being added as an interface configuration command to the Cisco 1600 series router asynchronous interfaces.

- CSCdk77783

  The Cisco 1005 router and Cisco 1600 series routers do not properly support the **ignore-dcd** serial interface configuration command. The Cisco 1005 router does not accept the command at all, and the Cisco 1600 series router accepts the command but does not operate properly if it is issued. Certain external modems and CSU/DSU devices require the ability of the DTE to ignore the DCD signal, and use of such devices is not possible until this fix is available. There is no workaround.

- CSCdk78895

  A Cisco router might experience a software-forced reload every one or two hours. This condition is caused by SNMP.

  Workaround: Do not use SNMP.

DECnet

- CSCdk65997

  This problem is specific to the Route Switch Module (RSM) platform and for DECnet over VLANs. The code for DECnet support over VLANs uses a cache to store VLAN-header information, and this cache is used in the fast-switch path. When there is a routing topology change, the fast-switching code continues to look at the stale cache entry, and as a result, packets destined by way of the new route are black-holed.

  Workaround: Disable DECnet fast switching on the relevant interface.

IBM Connectivity

- CSCdk30352

  Cross-domain session drops might occur when you configure **stun-tg** on Cisco routers to connect two FEPs. At the time the session drop happens, the following error might be reported by the router:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done may be reported by the router
  ```

  There is no workaround.

- CSCdk35420

  APPN HPR over an ISDN backup line is losing sessions. There is no workaround.

- CSCdk36470

  The input queue on the Token Ring interfaces might overflow and accept no additional packets.

  Workaround: Increase the input queue of the interfaces (for example, issue the **hold-queue 200 in command),** or reload the router.

- CSCdk53603

  When running DSPU, certain downstream connections might fail to become active.

  Workaround: To get the clients to become active, you need to clear the logical unit (LU) on the host that has the “PBIND” status. Once this is cleared, the session comes up.

- CSCdk67010

  There might be an SDLC DLSw performance problem when you use simultaneous full-datamode or simultaneous half-datamode. There is no workaround.

- CSCdk68763

  The ABM bit is not set on the transmitting DLSw peer during XID exchange. There is no workaround.

- CSCdk69202

  APPN builds fail because of an outdated compiler in the “dlurdepends” make file (dlurdepend.mak). All APPN images are affected. There is no workaround.

- CSCdk69510

  A DLSw router using priority peers might reload when the TCP peer connections fail under heavy load conditions.

  Workaround: Remove the Priority keyword until the issue is resolved.

- CSCdk71062

  When using privileged-level commands to allow configuration of a command, the user is unable to configure specific privilege levels for the keywords of the channel interface subcommand commands. There is no workaround.

- CSCdk77166

  A Cisco router that runs DLSw with FST, Direct, or LLC2(Lite) encapsulations might reload.

  Workaround: Use DLSw with TCP encapsulation.

- CSCdk87750

  An APPN HPR router might reload or issue a spurious memory access with the following backtrace elements when an APPN RSRB link is activated:

  ```
  0x60b1e590:anr_build_srb_map(0x60b1e400)+0x190
  0x60aff784:ncl_send_fastswitch_enable(0x60aff704)+0x80
  0x60afe458:ncl_populate_anr(0x60afe0f4)+0x364
  0x609ca31c:send_populate_anr(0x609c9f24)+0x3f8
  ```

  There is no workaround.

Interfaces and Bridging

- CSCdk20550

  The 10 Mbps full-duplex capability of the Cisco 3600 series NM-1FE-TX in Cisco IOS Release 11.2 P does not operate properly. The speed toggles between 10 Mbps and 100 Mbps. This affects the connectivity. There is no workaround.

- CSCdk23031

  Traffic cannot pass through a bridged interface when the encapsulation type is configured as Frame Relay (**encapsulation frame-relay**) and packet-by-packet compression is enabled. If packet-by-packet compression is not enabled, the problem does not exist. The root cause of this problem is that compression and decompression are not supported with bridging. (Refer to the following caveat: CSCdi63268.)

  Workaround: An earlier workaround was to disable compression in the source whenever bridging is enabled. Frame Relay encapsulation with packet-by-packet compression was apparently never taken care of. The solution is to disable compression whenever bridging is enabled. This can be accomplished with a check in fr_pbp_comp_decide(). If it is determined that bridging is enabled, do not set the compression flags.

- CSCdk53401

  When you netboot a Cisco 3640 router over the Fast Ethernet port, the Cisco IOS software proceeds to interactive setup without trying to load configurations from the network. This has been traced to an autonegotiation race condition where the Fast Ethernet port momentarily appears to be in a down state. There is no workaround.

- CSCdk60026

  A Cisco 2610 router configured with SDLC DLSw+ might not send SNRM to a terminal even though the status is “SNRMSENT” in the output from the **show serial interface** command. The interface shows “Link is UP, Line protocol is UP” despite the DTR being down.

  Workaround: Execute the **shutdown** command followed by the **no shutdown** command in configuration mode for the serial interface.

- CSCdk63173

  When ATM Lite tries to transmit a packet with multiple particles, in some applications such as L2F, particles after the third in the packet might not be 32-bit aligned. This causes the ATM Lite's transmitter to stall. Once this happens, issuing the commands **shutdown** followed by **no shutdown** gets the transmitter out of the stall state until the next such packet arrives.

  Workaround: Run L2F in process switching mode.

- CSCdk63201

  Multilink PPP disappears from the running configuration if SLIP is invoked. There is no workaround.

- CSCdk63464

  Priority queuing does not work for bridging when you are selecting frame types (access-list). Bridging traffic is forwarded to the default queue. There is no workaround.

- CSCdk63859

  Collisions and late collisions are seen when the Fast Ethernet interface is configured for full-duplex operation. The PHY was not getting reset after the duplex setting was changed through the management interface. Thus the interface continues to be in half-duplex mode while the peer is in full-duplex mode. This results in collisions or late collisions.

- CSCdk66019

  Under normal conditions, if **no keepalive** or **keepalive** *0* is configured on Fast Ethernet, the line stays up when the media-independent interface (MII) is removed or the cable is disconnected. However, if the interface is then reconfigured with **keepalive** *non-zero value* while the physical media stays down, the link still indicates that it is up.

  Workaround: Issue the **shutdown** command followed by the **no shutdown** command, or issue the **clear interface** command.

- CSCdk66320

  DECNET multicast packets might fail over VIP2 FDDI port adapters. There is no workaround.

- CSCdk74431

  A large packet might be corrupted if it is sent as a multilink PPP (MLP) bundle of two or more links with VPDN on an ATM PPP tunnel over an ATM-Lite interface.

  Workaround: Disable fasts witching on the ATM-Lite interface.

- CSCdk78561

  The Token Ring AR/FC bits are not set on the Cisco 2600 and Cisco 7200 series routers. Some PC applications require that these bits be set; thus, these PCs never connect. There is no workaround.

IP Routing Protocols

- CSCdj87730

  When NHRP is running in GRE multipoint tunnel mode, the router might reload if the IP address of the NBMA is learned from the same GRE tunnel cloud.

  Workaround: The workaround is to have the IP address of the NBMA learned from static route, or have the router learn it from a physical interface.

- CSCdj88650

  If OSPF has both an external and a summary route to the same network, and a partial SPF run deletes the summary route, the external route is not installed. The external LSA might have the routing bit set, even if it is not installed in the routing table. This is caused by a failure to reset the external's routing bit when the summary route replaces the external route in the IP routing table. The following sequence of events illustrates the problem, given external and summary routes to network 1.0.0.0:

  ```
  1. ospf installs external route to 1.0.0.0. The external LSA for 1.0.0.0 has its routing
  bit set 2. ospf installs summary route to 1.0.0.0, replacing the external route. The
  routing bit is not reset on the external LSA for 1.0.0.0. 3. ospf performs a partial
  spf to remove the summary route to 1.0.0.0. The external route to 1.0.0.0 is not
  installed. To add to the confusion, the routing bit is still set on the external LSA
  for 1.0.0.0.
  ```

  Issuing the **clear ip route *** command forces the installation of the external route. Alternatively, issuing the **clear ip ospf redist** command at the router that originates the external route triggers installation of the external route.

- CSCdk14556

  Occasionally a router in standby state responds incorrectly to a proxy ARP request. It puts the virtual MAC address in the ARP data field, which is correct. But it also puts the virtual MAC address in the MAC header, which is incorrect. The result is that a switch might associate the virtual MAC with the wrong port, and packets are no longer sent to the active router.

  If the active and standby routers are on different ports on a switch, the switch learns the virtual MAC address from both of them and might thrash its MAC layer cache.

  Workaround: Disable proxy ARP.

- CSCdk22030

  When there are many peers with many routes, some established peers might time out when a Cisco router is extremely busy. This condition might occur after you issue the **clear ip bgp *** command or after a reload. It might take more time for all the BGP peers to converge. This is a scalability issue.

  Workaround: Avoid the **clear ip bgp *** command if possible.

- CSCdk33769

  Under EIGRP, the command **distribute-list out** [*routing protocol*] does not work. The **distribute-list out** command does work without specifying the routing protocol option. There is no workaround.

- CSCdk34549

  A slow memory leak is seen in a BGP router running Cisco IOS Release 11.2(14)P. There is no workaround.

- CSCdk49790

  PPP peer neighbor routes from an unnumbered link might remain in the topology table when the link is down or changed to numbered. This condition causes instability in the network.

  Workaround: Remove the EIGRP process and reconfigure it, or reload the router.

- CSCdk60659

  The privileged clear access-template command fails if you use the wild card *any* as the address and network mask values. There is no workaround.

- CSCdk60926

  A Cisco router might fail when executing the **show ip route** *network* command. There is no workaround.

- CSCdk62939

  Removing a static route pointing to the null interface (or loopback) can cause EIGRP instability. There is no workaround.

- CSCdk63471

  Multicast assertion does not correctly prune router interfaces when no host reports are received from a VLAN. There is no workaround.

- CSCdk66969

  With synchronization and certain topologies, some BGP routes might not get advertised after peer reset.

  Workaround: Configure **no sync**, or **clear ip bgp** *x.x.x.x.*

- CSCdk67786

  NAT stops working once IP Cisco Express Forwarding (CEF) is turned on.

  Workaround: Do not turn on IP CEF.

- CSCdk72054

  A router might withdraw the summary and external LSA incorrectly after reboot.

  Workaround: Issue the **clear ip route *** command for summary LSA and issue the **clear ip ospf redistribution** command for external LSA.

- CSCdk73832

  IP EIGRP generates updates and causes high CPU utilization if more equal-cost paths than “max paths” are available. There is no workaround.

- CSCdk80809

  Some routes may not be propagated by EIGRP through redundant paths. There is no workaround.

ISO CLNS

- CSCdj89820

  ADMs have a low threshold on how much control traffic they can handle before resetting themselves. When a small number of ADMs reset themselves, the resulting type 4 TARP traffic is high enough that other ADMs reset themselves. The situation snowballs and the entire cloud cascades down into a TARP storm. There is no workaround. Once this starts, the only solution is to disable TARP on all the routers in the network.

- CSCdk17145

  When ISO-IGRP redistributes into IS-IS a routing entry might be duplicated, which results in a memory leak.

  Workaround: Reload the router to recover the lost memory.

LAT

- CSCdk57205

  Printing with LAT/TCP translation might produce an incorrect printout. There is no workaround.

Miscellaneous

- CSCdi72371

  When any Cisco 2500 series router is run with asynchronous/synchronous-capable 5-in-1 type connector low-speed serial ports in asynchronous mode, modem control is only supported when DTE-style 5-in-1 cables are used (in order to connect to DCE devices). The DCE 5-in-1 cable (in order to connect to DTE devices) does not support modem control for asynchronous mode.

  Workaround: Attach asynchronous DTE devices by using a DTE 5-in-1 cable and a null-modem adapter.

- CSCdk17210

  The Tx count is set to 1 when priority queuing (PQ) or WFQ is configured on the packet over E3/T3 (POET). This 34/44 Mbps interface performs poorly when fancy queueing is configured. There is no workaround.

- CSCdk27524

  When fax relay is used on a Cisco 2600 series router or a Cisco 3600 series router, some fax devices experience problems while sending large faxes (for example, more than five pages). The common symptom is that a fax in progress might experience retransmissions or possibly drop the call. This seems to be more of an issue with fax machines manufactured by Canon. There is no workaround.

- CSCdk28971

  A Cisco router cannot handle TCP flows according to the QoS weight defined after a reload or after using the **wr mem** or **conf mem** commands.

- CSCdk35200

  When CEF (**ip route-cache cef**) or DCEF (**ip route-cache distributed**) switching is enabled, a Cisco router stops sending ICMP redirects. This condition occurs when operating with Cisco IOS Release 11.1(20)CC through Release 11.1(21)CC. There is no workaround.

- CSCdk47375

  When a Kerberized Telnet is used to communicate between two Cisco routers, the credentials might not be forwarded. There is no workaround.

- CSCdk55236

  Modems that fail during trainup display the disconnect reason as “ATH detected.” Although a call is successful and is disconnected normally, the modem logs report the disconnect reason as “ATH detected.” There is no workaround.

- CSCdk59049

  When you run TRISL to a Cisco 7000 family router, some frames larger than 1535 bytes might not be forwarded. This condition occurs when you run TRISL between two VLANs that are on switches.

  Workaround: Do not use TRISL. Use an external device to route or bridge between the two different VLANs. Or modify the end devices so that they do not send packets larger than 1500 bytes.

- CSCdk59879

  A Cisco 1600 series router fails when IPSec is configured over an ISDN link. This is caused by the IP route-cache, which is enabled by default on all interfaces. Disable fast switching on the dialer interface and the router stops failing. However, TCP packets now get out of order. There is no workaround.

- CSCdk61860

  If the Cisco AS5800 access server router shelf reloads because of a software error, the system might not discover the dial shelf upon bootup.

  Workaround: To recover the system, reload the router shelf manually.

- CSCdk62331

  If an ATM permanent virtual circuit (PVC) is deleted on a point-to-point interface and a new PVC is created, and the new PVC has a different virtual circuit descriptor (VCD) than the old, Cisco Express Forwarding (CEF) drops packets that should be transmitted on that interface. The interface configuration commands **no pvc** followed by **pvc** produce this behavior, as does the **no atm pvc** *vcd* command followed by the **atm pvc** *different-vcd* command.

  Workaround: This can be corrected by issuing the **shutdown** command followed by the **no shutdown** command for the affected interface.

- CSCdk62487

  When non-distributed CEF is enabled after multicast routing is enabled, multicast packets are dropped.

  Workaround: Disable and then enable multicast routing.

- CSCdk62872

  SAR does not see the line pressure properly and overloads the multiplexing chip that causes cell drops for both UBR and CBR. There is no workaround.

- CSCdk64463

  When bridging is configured on an RSM VLAN interface that runs Cisco IOS Release 11.2P or Cisco IOS Release 11.3, NetFlow or optimum switching does not occur. When bridging is configured on an RSM VLAN interface that runs Cisco IOS Release 12.0, CEF switching does not occur. IP packets are processed by fast switching instead of flow/optimum/CEF switching, causing a significant decrease in the IP packet forwarding rate. The NetFlow Collector might also fail. There is no workaround.

- CSCdk65706

  When you turn off IP routing and reenable IP routing, CEF does not come on by default on some platforms (for example, the Cisco 12000 [GSR]). There is no workaround.

- CSCdk69045

  Custom queuing stops working completely as soon as rate-limit is activated. All queue counters show zero. Custom queuing can only be restored by reloading the router. There is no workaround.

- CSCdk69355

  Enabling tag switching with BGP and a full Internet routing table might cause a Cisco router to reload. The following message appears:

  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk
  ```

  There is no workaround.

- CSCdk70378

  When MPOA configuration is removed under moderate to heavy traffic across a LANE network, the RSM might crash. There is no workaround for this problem, except to not remove the MPOA configuration once it is operational.

- CSCdk71109

  When CEF is on, if an outgoing interface does not have CEF on (for example, SMDS encapsulation), packets are process-switched. This is due to lack of IP cache creation. There is no workaround.

- CSCdk71560

  Unencrypted traffic can suffer packet payload corruption when it flows through a Cisco router as encrypted traffic.

  Workaround: Turning off fast switching.

- CSCdk72452

  When an ATM uplink is broken or the remote CES sees loss of signal (LOS) or loss of frame (LOF), an alarm must be generated to the locally connected T1/E1 link. This condition sends alarm indication signals (all 1's) to all the timeslots configured in the structured mode. There is no workaround.

- CSCdk73672

  When an integrated access server is under extremely high traffic loads, some modems might be unable to answer incoming calls. This condition only occurs if the modems are set up to be autoconfigured.

  Workaround: Reenter the **modem autoconfigure type** command.

- CSCdk76192

  Packets that have the "do not fragment" bit set do not generate an ICMP unreachable packet when forwarded to an interface that requires the packet to be fragmented. This behavior is observed only with Distributed Cisco Express Forwarding (DCEF) switching mode on the Cisco 7500 platform. There is no workaround.

- CSCdk77426

  If a User Datagram Protocol (UDP) packet with an invalid length is sent to port 514 (the syslog port) on an IOS device, the device is likely to reload. In this situation, a stack trace might not be saved. Such packets are sent by the popular **nmap** port scanning program.

  Workaround: You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done by using either packet filtering on surrounding devices, or input access list filtering on the affected IOS device itself. If you use an input access list, that list should be applied to all interfaces to which attackers might be able to send datagrams. This includes not only physical LAN and WAN interfaces, but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and/or interface templates corresponding to GRE, L2TP, L2F, and other tunnelling protocols. The input access list must block traffic destined for any of the Cisco IOS device's own IP addresses, as well as for any broadcast or multicast addresses on which the Cisco IOS device might be listening. It is important to remember to block old-style "all-zeros" broadcasts as well as new-style "all-ones" broadcasts. There is no single input access list that works in all configurations. It is very important that you understand the effect of your access list in your specific configuration before you activate the list. The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply that access list. (The example assumes no need for input filtering other than as a workaround for this vulnerability.)

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0   0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

It can be complicated to list all possible addresses, and especially all possible broadcast addresses, to which attack packets might be sent. If you do not expect to receive any legitimate syslog traffic on an interface, you might wish to simply block all syslog traffic arriving on that interface. Remember that this affects traffic routed through the Cisco IOS device as well as traffic destined to the device. Input access lists have an impact on system performance, and should be installed with a degree of caution, especially on systems that are running very near their capacity limits.

- CSCdk77654

  An encryption session setup might not set up properly if the access list applied to a crypto map includes deny statements before permit statements.

  Workaround: Remove the deny statements in the access list. A ramification of the workaround is that more packets might match the encryption policy than were originally configured.

- CSCdk85273

  A Cisco 7505 router running Cisco IOS Release 11.2(15a)P with encryption "on" reloads when you perform an SNMP poll of the cieEngineStatusTable (from CISCO-IP-ENCRYPTION-MIB). This MIB object is queried by CiscoView, and might be queried by other network management tools. This behavior does not occur when encryption is "off."

  Workaround: Disable SNMP polling by removing all SNMP-server community statements from the configuration, or ensure that no management station polls for objects in the CISCO-IP-ENCRYPTION-MIB.

Novell IPX, XNS, and Apollo Domain

- CSCdk70331

  If an IPX access list applied to an interface with the access-group command does not exist, and at some later time an access list by that name or number is created, there is potential that IPX fast switching might forward packets that should be filtered.

  Workaround: When changing an access list, remove and then reapply that access list to that interface with the **ipx access-group** command. The cache should then be invalidated and rebuilt with the new access list rules. Alternatively, make sure the access-list is defined before the access group is applied to the interface.

- CSCdk75750

  Routing IPX between Bridge Relay Functions (BRFs) on an RSM running Cisco IOS Release 11.3(7)T does not work when IPX route-cache is enabled on the BRF interfaces.

  Workaround: Remove **ipx route-cache** from the BRF interfaces.

Protocol Translation

- CSCdk67626

  When you run protocol translation from TCP to X.25, it is possible to see high CPU utilization while minimal processes are running in the router. However, CPU usage goes down when actual work is being performed. This can be confirmed by issuing the **show process cpu** command at the enable prompt of the router. For example:

  ```
  Router# show process cpu
  ```

  This is a cosmetic problem. There is no workaround.

Wide-Area Networking

- CSCdj81263

  When IP fast switching is enabled on a Cisco 1600 series router with BRI interfaces, the router might fail if the ISDN connection is repeatedly brought up and down. For example, this condition occurs if the **clear ip cache** command is repeatedly invoked while the connection is being disconnected. There is no workaround.

- CSCdk07715

  According to all available Q.931 specifications, including that for the Northern Telecom Primary Rate DMS-100 switch, the "NOTIFY" message is only valid for call state 10 (call is active). The Cisco router was correctly rejecting calls in which this message was received in some other call state. However, some DMS-100 switches do send the "NOTIFY" message after a "CALL_PROC"

or “ALERTING” message while the call is in progress. The fix is for the router to allow but ignore the “NOTIFY” message, for the Primary Rate DMS-100 switch type only, in call state 3 or call state 4.

- CSCdk42597

  An incoming call does not route the called NSAP facility and calling NSAP facility on the outgoing side. There is no workaround.

- CSCdk42780

  A Cisco 3640 router rejects incoming calls even though there are free channels and good modems. Both ISDN and analog incoming calls are rejected with the following message:

  ```
  Incoming call rejected, exceeded max calls
  ```

  This occurs in the Cisco IOS Release 11.2(15.1)P image where the fix for a previous caveat (CSCdj77099) is already integrated. There is no workaround.

- CSCdk42813

  When running with multicast fast switching, small packets coming from a LANE subinterface that need to be mrouted to another LANE subinterface are not sent correctly. Runts appear on the Ethernet interfaces connected to C5k. There is no workaround.

- CSCdk55183

  In an environment where DLSw is running with Ethernet (local ack) attached end stations, the connection might be lost because of sequence number problems on frames sent by the router. This situation causes a Frame Reject (FRMR) message to be sent by the end station. There is no workaround.

- CSCdk60097

  On a Cisco AS5300 access server running Cisco IOS Release 11.3(6.1)T with an IP plus feature set, the global command **modem busyout-threshold** *xx* cannot place B-channels in service or out of service on an NFAS line without a D-channel (the line is neither a primary nor a backup NFAS line). There is no workaround.

- CSCdk61807

  When you perform an ISDN callback, you might receive the following message:

  ```
  %SYS-3-HARIKARI: Process ISDN top-level routine exited
  ```

  There is no workaround.

- CSCdk62967

  Cisco 2600 series routers with ISDN configurations, both Basic Rate ISDN (BRI) and Primary Rate ISDN (PRI) interfaces, can reload with a watchdog timeout when the ISDN interfaces are “active/operational.” This condition only occurs on Cisco 2600 series routers running Cisco IOS Release 11.3(6.2)T and later, Cisco IOS Release12.0(1) and Cisco IOS Release12.0(1)T.

  There is no workaround.

- CSCdk63462

  The expiration of a response timer (T200) can cause Layer 2 to disconnect and not reconnect until the router is reloaded. There is no workaround.

- CSCdk64220

  Test frames with a virtual Media Access Control (VMAC) address respond with the Burned-in MAC address (BIA) as the source address. This is a protocol violation. There is no workaround.

- CSCdk64929

  When you configure X.25-over-TCP (XOT) keepalives on the X.25 route statements, a router might restart with following (decoded) traceback:

```
c3640-js-mz.113-6.1.symbols read in
Enter hex value: 0x605FF664
0x605FF664:xot_update_keepalive(0x605ff644)+0x20
Enter hex value: 0x606094F8
0x606094F8:x25swt_verify_call(0x606092e4)+0x214
Enter hex value: 0x6060D880
0x6060D880:x25swt_process_incoming_call(0x6060d840)+0x40
Enter hex value: 0x6060D7CC
0x6060D7CC:x25swt_flagged_wakeup(0x6060d704)+0xc8
```

  There is no workaround.

- CSCdk65469

  A switch type TS014 numbering plan misidentifies the called number as “national” when it should be “unknown.” There is no workaround.

- CSCdk66109

  Under unusual circumstances that include protocol processing delays induced by debug reporting, X.25 switching operations can cause a Cisco router to reload. There is no workaround.

- CSCdk66393

  ISDN PRI switch type primary-ntt can get a slot map in Channel IE in an incoming Setup message. It should not include the “interface specifier” in Channel IE of the Call Proceeding message. There is no workaround.

- CSCdk66501

  Call control blocks (CCBs) are not properly cleaned up on a Cisco 7500 series router with multiple PRIs. Multiple CCBs are assigned to a single B-channel on a PRI after you issue the **show isdn status** command. This might cause the router and ISDN switch to get out of synchronization with regard to the available B-channels. This condition might cause a user to fail to connect, with the failure reason being “Requested channel not available.” There is no workaround.

- CSCdk67475

  Under heavy usage conditions on an X.25 serial link, a Cisco router running translated X.25 to virtual asynchronous connections (PPP/IPX) might reload. This appears to be an infrequent occurrence. There is no workaround.

- CSCdk67735

  VPDN does not support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

  Workaround: Use CHAP or PAP.

- CSCdk70026

  A status message with “endpointRef” is not processed in the multipoint state table. This could result in releasing a multipoint virtual circuit. There is no workaround.

- CSCdk76492

  Under heavy call connection and disconnection activity, the system might restart because of a software error. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(2)

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(2). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdk09732

  R2 signaling is failing in Croatia. According to the ITU specification (page 60 Note II), the router needs to act on the SEIZURE signal between 100 to 200 msec. This occurs around 150 milliseconds, within specification. However, for Croatia it has been confirmed by the switch manufacturer as well the PTT HPT, that the typical value needs to be 50 msec, maximum 60 msec.

- CSCdk20217

  On Cisco AS5200 and Cisco AS5300 access servers, assertion failures can result in the servers failing.

- CSCdk30581

  An access server might fail when a MICA device runs out of buffers (prints out NO_BUF messages on the console) and a lot of EXEC sessions are running. This problem has been observed with the latest 56K modems.

- CSCdk36682

  A Cisco AS5300 access server might fail to place a call and issue the message “no signalling channel is available for outgoing call” because of certain sequences of **shutdown** and **no shutdown** on T1 controllers, if controllers have both CAS and PRI configured. The workaround is to always configure **no shutdown** on controllers with CAS first.

- CSCdk38665

  When you configure a channel group, unconfigure the channel group, and then configure a PRI group with Cisco IOS Release 11.3 T and later, a bus error occurs.

- CSCdk39751

  The failed call count does not include unanswered calls.

- CSCdk62405

  The **absolute-timeout** line configuration command does not accept a value for the timeout parameter.

AppleTalk

- CSCdj72157

  AppleTalk subinterfaces on SMDS return the wrong SMDS address when an AARP request is sent. The router returns the SMDS address associated with the first subinterface regardless of which subinterface is associated with the AARP request.

- CSCdk38556

  Disabling a subinterface turns off AppleTalk route-cache for all subinterfaces on that interface.

  Workaround: Enable the subinterfaces’ AppleTalk route-cache after disabling one of the subinterfaces by issuing the **interface** *subinterface* **appletalk route-cache** command.

Basic System Services

- CSCdj78490

  Cisco 1003 routers sharing S bus frequently have problems. Even though diagnostics show that the router is responding to IDCKREQ from the ISDN switch, these responses are lost in collisions and never seen by the ISDN switch.

- CSCdk08376

  LANE clients might drop with the message “SNMP CPUHOG processing GetNext IfEntry” on the ATM subinterfaces. In some cases, numerous subinterfaces were defined, which were not numbered sequentially. A partial workaround is to issue the command **no snmp-server sparse-table**, which lessens the frequency of occurrence.

- CSCdk09806

  When configuring traffic-shape groups under interfaces, the second traffic-shape group does not show in the running-config or startup-config if options are not added to the command as the first statement.

- CSCdk11908

  A Cisco 1005 router might report the following message repeatedly:

  ```
  %ETHERNET-1-TXERR: Ethernet0: Fatal transmit error. Restarting... %QUICC-5-COLL: Unit
  0, excessive collisions. Retry limit 15 exceeded
  ```

- CSCdk24065

  A router might fail and display this bus error:

  ```
  System was restarted by bus error at PC 0x6013425C, address 0xD0D0D6D
  ```

- CSCdk27388

  There might be a problem on the VIP with regard to fragmentation of packets that can cause the DMA engine to stall (and cause the VIP to fail). The message “DMA receive error” might be displayed. There is no workaround.

- CSCdk33632

  Under noisy line conditions a giant packet followed by a runt packet on a serial line causes a Cisco 2600 series router to fail.

- CSCdk36156

  A router becomes unresponsive when a query router history is attempted and the history table is empty.

- CSCdk38758

  With RSP HSA, issuing the command **write memory** might not correctly update the ROM monitor boot variables on the slave processor.

  Workaround: Verify that the BOOT variables have been correctly written by issuing the **show bootvar** command on the master after every **write memory** command, and reissuing the **write memory** command as many times as necessary.

- CSCdk39738

  After a user dials in to a Cisco AS5200 access server and is passed to the TACACS+ server, and is authenticated, the access list that is passed back to the router by the TACACS+ server is not applied to the asynchronous interface by the router. There is no workaround.

- CSCdk40393

  A Cisco MC3810 with both multiflex trunk (MFT) and digital voice module (DVM) installed might see T1 clock slips on the T1 controllers under certain circumstances. Clock slips are reported when viewing the T1 controller statistics with the EXEC command **show controller t1**.

  When the Cisco MC3810 is configured with both T1 controller 0 and controller 1 set for **clock source line** and the proper global configuration command **network-clock-select** has been entered, the Cisco MC3810 system clock synchronizes with one of the T1 controller clocks while temporarily setting the other controller to loop timing. The problem is that even though the secondary T1 controller reports loop timing as seen with **show controller t1**, the system clock is still being driven by both T1 controllers. This occurs even though there might only be one active T1 line connected to the Cisco MC3810 or even when the unused T1 controller is administratively shut down.

  The workaround for this problem is to set one of the controllers for either loop or internal through the controller subcommand **clock source**.

- CSCdk40554

  Crash information might not be saved when certain types of memory corruption occur.

- CSCdk40599

  An SNMP memory might leak when SNMP ping is enabled.

- CSCdk41472

  Using traffic shaping with custom queuing might drop too many packets.

- CSCdk41494

  If a network management application were to add an entry in the ping MIB table, not activate the entry, and then delete it before it is aged out of the MIB by the 5-minute timer, the router could fail.

- CSCdk41795

  The **aaa accounting nested** configuration command is not available from the configuration parser.

- CSCdk42462

  X.25 CSTATE occasionally runs out of stack space, causing an unscheduled reload of the router.

- CSCdk43920

  From the login prompt, it is possible to recover fragments of lines typed by the previous user of the same physical or virtual terminal line. This might represent a security exposure. A complete description and details are at http://www.cisco.com/warp/public/770/ioshist-pub.shtml.

- CSCdk44323

  A router is not able to connect to the mainframe, if the mode-name is less than eight characters.

- CSCdk45166

  Timeslot 1 appears to get into a hung state at the framer level and endlessly sends a ABCD=F. This is only seen when you do a tdm-group and a cross-connect for timeslots 1 through x.

- CSCdk47382

  NTP on Cisco 2600 series and Cisco 3800 series platforms does not stay synchronized. After some time, the clock wanders and NTP becomes unsynchronized. Removing the NTP configuration and adding the NTP configuration back causes the router to synchronize again, but later it becomes unsynchronized.

  Workaround: Issue the **ntp clock-period 17208078** command.

- CSCdk51491

  If a router is configured to support Layer 3 switching with in and out access filters on the HSSI and Frame Relay IETF encapsulation, subsequently trying to configure SMDS encapsulation causes the router to fail.

- CSCdk53176

  Issuing the **no traffic-shape group** command causes the router to fail.

- CSCdk55115

  V.120 users can now correctly configure **autocommand ppp negotiate** under vtys.

- CSCdk57493

  Starting with Cisco IOS Release 11.3(5.1)T, a reverse-Telnet connection that receives a Telnet BREAK sequence fails to send an EIA/TIA-232 (RS232) BREAK to the associated async line. An outgoing Telnet connection that receives a Telnet BREAK sequence also fails to output a BREAK condition; this instance of the problem has existed for quite some time.

- CSCdk64322

  RSP range registers set correctly to enforce the 2-MB limit on MEMD access.

EXEC and Configuration Parser

- CSCdk33946

  The router might fail while editing the command line under low memory conditions.

- CSCdk52457

  Using ctrl-x to terminate a Telnet connection might cause the router to fail.

IBM Connectivity

- CSCdk10830

  An APPN router might display a single console CP-CP session. This CP-CP session cannot be deactivated by issuing the **appn stop cp-cp** command.

  Workaround: Stopping the APPN link clears this problem.

- CSCdk12302

  While control units are being removed by router or end device activity, issuing the **show bsc** command might cause the router to fail.

- CSCdk25935

  While DLSw with FST encapsulation is configured on a router, the following error message with traceback might appear:

  ```
  00:39:38: %SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=ADDD9C -Traceback= 148D3A 572A 4DF4
  110064 17DAA2 17B0DA 14CC 10005B4 10047DA
  ```

- CSCdk36264

  If DLSw is configured to use TCP as the transport, and if the following conditions are met, a TCP packet coming from the peer could get stuck in the TCP buffers of the router. A TCP packet might get stuck when there are no keepalives between the peers (like in an ISDN connection), there is no

heavy traffic between the peers using the DLSw pipe, and a packet coming from the peer is 1 to 3 bytes in excess of the MSS (Maximum Segment Size) of the receiver. Under these conditions, the receiving TCP device does not give the assembled packet to DLSw, until another packet arrives.

Workaround: Adjust the MAXDATA (MAX PIU) of the end node to the value of MSS-16 bytes (allowing 16 bytes for the DLSw header) in the case of SNA.

- CSCdk37560

  A Token Ring LEC configured for HSRP and multiring IP might respond to IP RIF packets received from the BUS, even though it is not the intended recipient for such packets. This happens when IP packets with a RIF are sourced by other LECs on a Token Ring ELAN and targeted at remote devices which are one or more SRB hops away from the ELAN. The LEC fails to filter these packets, thereby causing IP looping problems in Token Ring LANE environments. This problem occurs on the Cisco 4700, Cisco 7200, Cisco 7500, and Cisco RSP7000 platforms.

- CSCdk39734

  APPN auto-activate on demand works only once in Cisco IOS Release 11.2 and does not function at all in Cisco IOS Release 11.3. There is no workaround.

- CSCdk41016

  The router fails when BSC receives a frame through BSTUN while it is in the process of transmitting a frame on the BSC line.

- CSCdk41218

  When Bisync is running on a branch router connected to an NCR5085 cash machine, if a corrupted acknowledgment is received from the ATM XA machine, under unusual conditions you might see the input queue on the serial interface connected to the ATM machine get into a wedged state. If the serial interface is in this state, issuing the **show interface** command displays the value of input queue as 75/75.

  Workaround: Shut down the interface and bring it back up by issuing the command **shutdown** followed by **no shutdown**. An additional workaround is to schedule the **shutdown**/**no shutdown** by increasing the interface input hold queue size by issuing the command **hold-queue 150 in** under the bisync interface.

- CSCdk46217

  A Cisco 2600 series router running Cisco IOS Release 11.3(5)T and later, configured for BSTUN/Frame Relay, might lose a portion of the Frame Relay configuration and the encapsulation might change from Frame Relay to BSTUN. (You can see that the configuration has changed by issuing the **show interface** command.) This causes the Frame Relay link to go down when the router is reloaded. There is no workaround.

- CSCdk48387

  A Cisco 4500 router configured with a Token Ring LE Client adds 6 extra bytes when fast switching routed protocol packets from a Token Ring LEC ATM interface to the packets' target (output) interface. Although this problem is known to occur with IP packets, it potentially exists for other routed protocols that are fast switched in from a Token Ring LANE interface and fast switched out to the packets' target interface.

- CSCdk53320

  An APPN router might reload with the following traceback error in the **show stacks** log capture:

```
%APPN-3-Error: INVALID LPID 61318C81 Pid 0020100C IPSname 1
-Traceback= 608E1EF0 608DAF04 608DB440 6081184C 60810D40 601D4EA8 601D4E94
%APPN-6-LogMsg: APPN Process ended abnormally. Name: psp00. RC: F0AA0000.

System was restarted by error - a Software forced crash, PC 0x601EED8C

Stack trace from system failure: abort(0x601eed84)+0x8
crashdump(0x601ed76c)+0x18
Pexit(0x608dc608)+0x88 LP_lpid_deallocate(0x608db3e8)+0x68
psp01b(0x608117b0)+0x9c psp00(0x60810b10)+0x230
```

- CSCdk54077

  An APPN router might reload with a SegV exception in psp00 after the following message is displayed in a rare race condition:

```
%APPN-6-APPNSENDMSG: APPN Allocate 613D1F8C to NETA.MVS1 timed out for TP “001.

System was restarted by error - a SegV exception, PC 0x606AE270
```

- CSCdk54687

  An APPN router enlarges its LFSID table from a small model to a large model if more than 12 SIDLs are active for a specific SIDH. The large LFSID table requires substantially more memory.

  The resolution to CSCdk54687 increases the number of entries in the small LFSID table to the maximum number of SIDLs that fit into this table. This requires no additional memory per link but increases the number of SIDLs supported in the small LFSID table. Thus, in customer networks that typically support 17 LUs/PU, the APPN router might use significantly less memory.

- CSCdk55765

  DLUR routers incorrectly update the max-BTU-size for links to Type 2.1 nodes.

Interfaces and Bridging

- CSCdj43445

  The FDDI port adapter now has a software address filter at the VIP level to filter out unwanted multicast packets. This helps performance and also unnecessary entries in NetFlow tables.

- CSCdj85213

  A router coded as a primary SDLC interface might send an erroneous frame, causing the secondary device to send a FRMR.

- CSCdk01309

  When a 100-Mbps interface on the Cisco 3600 series, configured for ISL encapsulation, is modified, the interface might cause carrier loss and ISL trunk flapping.

- CSCdk10225

  When you attach some routers, such as a Cisco 2500 series or Cisco 4000 series router, directly to a switch that is configured for autosense, the switch detects the port as being full-duplex, but the routers only support half-duplex. The Token Ring interface on the router shows up/up but only broadcast traffic passes. On the switch you see line errors incrementing at a very high rate. A ping issued from the router to a local device on the ring with the switch fails.

  Workaround: Manually set the switch to half-duplex.

- CSCdk10762

  After a reboot, or CBUS complex restart, there is a small chance (one in several thousand) that one or more T1s in a CT3 IP will not come back up properly. There are a very specific set of symptoms for this failure:

  – The line comes up at both ends, so all is well physically.

  – No T1 alarms or performance monitoring errors are detected.

  – The line protocol is down (assuming keepalives are enabled).

  – The far-end router counts large numbers of CRC errors in its relevant **show interface** counters.

  – The near-end router (that is, the relevant CT3IP interface) does not show any errors in its counters.

  – The T1 number is 1 through 20 (T1s 21 through 28 are not affected by this problem).

  Once in this state, issuing the command **microcode reload** or reloading the router is the only way out of this state.

  All Cisco IOS releases that support CT3IP have recently been modified to include more details in the hardware version string displayed in the output of the **show controller t3** command. Prior to firmware version 2.8.0 this display would merely show a H/W Version of 5 as seen in this example:

```
router# show cont t3 0/0/0
T3 0/0/0 is up.
  CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.7.0
```

  After upgrading to a Cisco IOS image that includes firmware version 2.8.0 or later, the above display is enhanced to include more hardware version details as seen in these two examples:

```
router# show cont t3
T3 0/0/0 is up.
  CT3 H/W Version : 5.0.0, CT3 ROM Version: 1.2, CT3 F/W Version: 2.8.0
```

```
router# show cont t3
T3 0/0/0 is up.
  CT3 H/W Version : 5.0.1, CT3 ROM Version: 1.2, CT3 F/W Version: 2.8.0
```

  Hardware versions 5.0.0 and 5.0.255 are subject to this caveat. Hardware version 5.0.1 is not. (If you see a hardware version of 5 with no additional numbers, update your software to a more recent version).

- CSCdk11808

  Certain types of terminal adapters (for example, NEC) might toggle many control lines during the DTR pulsing. These line status changes interrupt the port adapter 8T/4T+ controller and cause a reset of the line by the IOS driver. Thus the DTR pulse is shortened.

- CSCdk18176

  A router with bridging enabled on an ATM Interface (AIP) might continually reboot. A router at the end of the PVC might fail with a software forced failure. This caveat was first identified in Cisco IOS Release 11.1(18.1)CA.

- CSCdk31994

  Beginning in Cisco IOS Release 11.3(4), a Cisco 4500 router configured for SRB might not remove IP frames from an FDDI ring. This causes IP frames to circulate around the ring until the TTL expires. This problem is seen when two or more Cisco 4500 routers are configured for SRB on the same ring.

- CSCdk36767

  EIP interfaces on a Cisco 7500 series router running Cisco IOS Release 11.2.13 starts flapping and then goes into an up and down state. Issuing the **shutdown** command, followed by the **no shutdown** command does not bring them back. You must do a microcode reload to stabilize the box. Or a reload of the box also normalizes the status.

  Workaround: Perform a microcode reload periodically (every day during maintenance time period), or upgrade EIP microcode to latest version

- CSCdk39102

  Beginning with Cisco IOS Release 11.3(5.1), a Cisco 1600 series router configured with Frame Relay encapsulation might fail in Frame Relay compression (FRF.9).

- CSCdk39193

  HSSI3 H2T microcode does not RX/TX unless both RX/TX clocks are present, because the HSSI3 code waits for the a chip reset to be done at the beginning of the code. However, chip reset is only done at boot time or during online insertion/removal (OIR).

- CSCdk39936

  Fast Ethernet port adapter full-duplex interfaces bounce up and down when configured in Fast EtherChannel (FEC). A workaround is to use the port adapters in half-duplex mode when they are FEC members or unconfigure FEC.

- CSCdk44597

  The PA-A1 ATM adapter cannot transmit OAM cells. There is no workaround.

- CSCdk46966

  If CEF switching is enabled and an IP address is assigned to an ISL subinterface, if the subinterface is deleted but the same IP address is assigned to another interface, the router can fail.

- CSCdk51723

  Under some circumstances the PA-A3 might cause an RSP restart with an output stuck message.

- CSCdk57555

  A Fast Ethernet interface might hang under extreme traffic stress on a Cisco 7200 series router when used with ATM interface.

- CSCdk57624

  When CEF switching is enabled and Fast Ethernet interfaces are configured for flow switching, CEF-flow switching fails on FEIP, if ISL is configured. Packets are fast switched instead. There is no workaround.

- CSCdk58799

  When using CiscoWorks to manage a PA-MC-T3, it is mistakenly represented by CT3IP.

- CSCdk62768

  A Cisco 3600 series router might not send keepalive messages when keepalive is set.

IP Routing Protocols

- CSCdk05172

  After issuing the command **no distance eigrp 255 255**, the inaccessible routes might not be restored to the routing table. A workaround is to issue the command **clear ip eigrp neighbors** on the interfaces of the affected routes.

- CSCdk12537

  A router running Cisco IOS Release 11.3(3) and later, configured with a policy route map on a BRI interface, might not forward packets to the next hop as specified in the **set ip next-hop** command.

  The following conditions must exist for policy routing to fail:

  – **ip policy route-map** *name command* is configured on a BRI interface

  – the destination exists in the IP cache table of the policy router

  Workaround: Issue a **clear ip cache** command, or remove fast switching by issuing the **no ip route-cache** command.

- CSCdk26313

  NetBIOS over TCP/IP port 139 is not getting translated.

- CSCdk26388

  The router displays console error messages during periods of high serial line utilization. Error messages are of the form:

  ```
  %SYS-3-CPUHOG: Task ran for 2672 msec (87/71), Process = IP Input
  ```

- CSCdk26867

  On a Cisco 2600 series router running the c2600-is-mz_113-3a_T1 image and the NAT protocol, NAT works until the translation table times out. Only a reload of the router every 24 hours resolves the problem.

- CSCdk28025

  Routers with equal cost (redundant) paths between two Enhanced IGRP neighbors might experience problems with redistribution of static routes with a specified next hop. This problem only affects redistribution of static routes with a next hop specified and equal cost links with the next hop on one of the links. The interface connected to the same net as the “next hop” must come up after the redistribution in order to see the problem.

  Workaround: Issue the **clear ip route *** command.

- CSCdk29300

  DVMRP prunes received over a point-to-point link other than a tunnel, are silently ignored when they are sent to a unicast address.

  Workaround: Build a tunnel with the DVMRP neighbor.

- CSCdk40372

  The command **clear ip route** *net* removes a connected route from the routing table which will not be properly reinstalled. This is a regression introduced in 12.0 by CSCdk01482

  Workaround: Issue the commands **shutdown** followed by **no shutdown** if the net is lost.

- CSCdk43485

  If a received update has an as-path loop and/or any other bad attribute (for example, bad nexthop), when running under soft reconfiguration inbound, the clean copy of the paths is left around (received-only). This brings back the denied path if the command **clear neighbor soft in** is issued, and might alter path selection.

- CSCdk43575

  A packet translated by NAT in the fast path might fail input ACL check if it is bumped for process switching.

- CSCdk45874

  A Cisco MC3810 reloads with the error “CPU exception: reason = FORCE_CRASH(959fd4)” if policy routing is configured.

- CSCdk47222

  Beginning in Cisco IOS Release 11.3(5) and 11.3 (5)T, DNS A RR responses will be dropped by NAT, if the packet is going from NAT outside to NAT inside, and the inside source mapping has an access-list which permits any, and the embedded IP address is an OUTSIDE GLOBAL address.

- CSCdk47229

  If you have demand circuit (including virtual links) and external LSAs on a router, the router fails within 20-25 minutes.

  Workaround: Do not to use demand circuit and virtual links.

- CSCdk57195

  When the number of (S,G) entries for IP multicast routing goes above 2730, the line card of GSRs or the VIP card of an RSP might reload due to memory corruption.

  The symptom of this bug is a repetitive pattern of unicast address, multicast address, followed by four long words (usually holding zeroes or very low count) in corrupted memory blocks.

  The following records are other instances of the same caveat:

  – CSCdk47461 vip redzone crash

  – CSCdk48461 Software forced reload at SYS-6-MTRACE: mallocfree

  – CSCdk58110 VIP crash with SYS-3-BADBLOCK: Bad block pointer 603D6058

  – CSCdk60767 Memory corruption in get_buffer

  This router reload does not happen in images which have the CSCdj87399 fix.

- CSCdk58728

  A BGP session might be reset when the same password is re-applied to the session. Also, password configuration for a peer-group might reset all the sessions of a box. There is no workaround.

- CSCdk61629

  DNS NS records that have glue records translated have the TTL of the glue records set to 0. The TTL of the NS record is not set to 0. Thus the DNS server has an NS record for a DNS zone but no glue records. The next time the DNS server needs to contact the remote DNS server it fails because it has a NS record cached but no IP address to reach it.

- CSCdk62935

  Static routes for 0.0.0.0 do not redistribute into other routing protocols.

  There is no workaround.

- CSCdk63163

  If the **ip pim send-rp-announce** command is configured when a router runs out of memory, the router might fail.

  Workaround: Unconfigure this command if the router is known to be at risk of running out of memory.

ISO CLNS

- CSCdk37556

  A router might fail if the **distribute-list out** command is configured with IS-IS as the routing protocol. For example:

  router *protocol* **distribute-list** *acl* **out isis**

  This failure can occur when configuring any IP routing protocol.

  The **distribute-list** command does not work with IS-IS, so the specification of IS-IS routing protocol in the **distribute-list** command is invalid. The failure occurs because the invalid input is not handled correctly.

  Workaround: Avoid specifying IS-IS routing protocol when configuring the **distribute-list out** command.

LAT

- CSCdj38034

  A Cisco router running Cisco IOS Release 11.1(12) and later, fails at hi_delete, hi_open and lattcp.

Miscellaneous

- CSCdj29595

  If two Cisco 7500 series routers are connected to many Ethernet interfaces with EIP interface processors, and are running HSRP on many of these interfaces, the HSRP configuration might take several minutes to determine the active and standby routers after a router reloads. During this period of instability, the CPU load on the router approaches 100 percent.

  Workaround: Replace the EIP interface processors with VIP interface processors and Ethernet port adapters. A less effective workaround is to reduce the number of HSRP groups, or to increase the HSRP hello and hold time. Cisco recommends using no more than 24 HSRP EIP interfaces. VIPs have been approved at 80 HSRP interfaces.

- CSCdj87399

  CPU intensive tasks like OIR, or commands like **config net**, and **debug**, that print a lot of output have provoked router failures in some customer installations. It is believed that a high background CPU load can also provoke the failure.

  A software forced failure occurs because of a process watchdog timeout in ipc_cbus_process(). The IPC input process, ipc_cbus_process(), was not suspending until it had drained its entire input IPC message queue. This resulted in the process running too long, and suffering a process watchdog timeout.

- CSCdk01958

  The **full-duplex** command does not work on the 1FE PA. There is no workaround.

- CSCdk05355

  The **logging synchronous** command can cause logging to stop. The recommended workaround is to remove this command.

- CSCdk08850

  A PA-T3 port adapter might go into loopback after a router reload. A workaround is to issue the commands **shutdown** followed by **no shutdown**, or the **clear interface** command.

- CSCdk17038

  The router reloads when configuring the **crypto key** and **named-key** commands. The router boots up after the reload, but it does not load the configuration from NVRAM even though the configuration register is set to 0xE002.

- CSCdk19122

  The CT1-PA and CE1-PA, when configured with the **compress stac** command, in a system with a CSA-PA (hardware compression PA), experiences memory leakage in the pool manager. When available memory goes down to a low value (less than 1M), the router fails.

  There is no real workaround. However, unplug CSA-PA from the system and software compression will be used instead. There is no memory leak with a CT1-PA and software compression.

  On a Cisco 7500 series router, this causes the output to be stuck.

- CSCdk19805

  When you Telnet into one router, then from that router to another, and if both Telnet sessions are encrypted and kerberized, then the second Telnet console might receive garbled characters. The commands entered in this session take effect on the second router, but their output is illegible.

- CSCdk23648

  When multiple KDCs were configured, there was no way to control the timeout such that failover can occur. This caused common client applications to fail before the next KDC is contacted. There is no workaround.

  To resolve this caveat, the following two commands were added:

  kerberos timeout *seconds*—Communications with the KDC uses this timeout. The range is from one to ten seconds, and the default is 5 seconds.

  kerberos retry *retries*—Communications with the KDC will retry this many times. The range is one to five retries, and the default is four retries.

  These commands show up in the configuration when not set to their default values.

- CSCdk23751

  Attempting to encrypt to a phantom router causes memory leaks.

- CSCdk24418

  Sometimes the modemcap defined for a modem might not be applied to the modem before allocating the modem for a new call.

- CSCdk26869

  Various reloads pointing to inspect option of Cisco IOS firewall.

- CSCdk29115

  If Bisync is configured (**encapsulation bstun** command) with ASCII characters (**bsc char-set ascii** command) on the first port of a serial WIC (1T, 2T or 2A/S) in WIC slot 0 of a Cisco 2600 series, only the first character of each frame is received, and the BSTUN tunnel does not get established. Other encapsulations are not affected, and using the EBCDIC character set with Bisync works correctly.

  Workaround: Use a different serial port: either the second serial port (port 1) on a 2T or 2A/S WIC in WIC slot 0 or any serial port in WIC slot 1. If you have only one serial WIC, moving it from WIC slot 0 to WIC slot 1 corrects this problem.

- CSCdk34205

  If you are using NFAS with a backup D-channel and the primary D-channel goes down, modem calls might fail to be accepted into the access-server. Enabling the **debug modem csm** command displays the “dchan_idb state is not up” error message.

- CSCdk34893

  A router fails right after the user configures an S/T BRI interface into the 128-kbps leased-line mode. There is no workaround.

- CSCdk34968

  After 32767 encryption connection setup attempts, encryption connection setups might not complete.

  Workaround: Reload the router.

- CSCdk35745

  CBAC fails to create the dynamic ACLs to allow the establishment of FTP data channels if the FTP client sends command terminated with a single carriage return character (instead of carriage return and linefeed characters). The symptom of this problem is that the FTP client hangs after issuing commands that require the exchange of port (to set up a data channel between client and server) like ls, get and put.

- CSCdk38133

  The **cablelength** configuration command for the CT1 module is missing in the Cisco 2600 series router for Release 11.3 T.

- CSCdk38459

  On a Cisco 2600 series router issuing the commands **shutdown** followed by **no shutdown**, or **clear interface bri**, to a BRI interface on the MBRI-NM does not bring up the ISDN D-channel layer 2. The ISDN layer 2 shows that it attempts to send the line setup frame, but reports that the other end does not respond correctly. This is because the interface hangs and there are no more frames transmitted.

  Workaround: Do not issue these commands. If the interface needs to be reset, the router needs to be reloaded.

- CSCdk39728

  If an interface is configured for both NAT outside and encryption, all incoming packets targeted at the router are forced to the encryption engine, regardless of whether or not they are (or should be) encrypted. All non-encrypted packets are then dropped by the encryption engine.

- CSCdk39922

  When attempting to dial out on a Cisco 3600 series router using the digital modems and a single port T1 network module, the outbound call fails with “No Answer”. Inbound calls function correctly. Outbound dialing with T1 CAS and a dual-port T1 network module works correctly.

- CSCdk40114

  If the TCP keepalive timer is configured, the router might fail in random places in the TCP stack due to corruption of the TCP control block.

- CSCdk40947

  When the link(s) between redundant ATM ARP servers breaks, then the ARP servers keep trying to contact each other to repopulate the ARP cache.

  Due to excessive signalling the CPU load on the routers and ATM switches can rapidly reach 99%.

  The workaround is to use only one ARP server or to put them on very stable links.

- CSCdk41708

  There is a limitation of 25 encryption maps on an any VIP. This limit is likely to be reached when encrypting many serial lines on the VIP using a fractional T1 or E1 port adaptor.

- CSCdk41735

  When the traffic between the PA-12E/2FE port adapter and the CPU is high and the PCI bus is overloaded, a DEC21140 can get “underrun” and “overrun” errors. This is due to PCI congestion. The traffic is affected momentarily, then restored.

- CSCdk42816

  An Ethernet interface running Tag Switching and CEF might get into a state where the IP packets are not forwarded properly. The problem occurs when a CEF entry is improperly pointing at a Tag data structure. To check whether this is the problem, issue the command **show adjacency detail** for the next hop on the failing route. In the failure case, the packet counts on the IP adjacency will not be increasing, but those on the TAG adjacency will.

  Workaround: Disable Tag Switching on the interface.

- CSCdk42845

  On run-from-Flash systems, issuing the command **copy flash tftp** incorrectly invokes the Flash load helper code.

- CSCdk42920

  In some situations, FTP file transfers would fail due to an internal error.

- CSCdk43602

  Bell 103 communication does not work on the analog Microcom modems in answer mode.

- CSCdk44137

  The Explorer bit, in the TRISL header, might be incorrectly set for Non-Specific Routed (NSR) frames. Normally, the Catalyst 5000 and 3900 ignore this bit for NSR, but sometimes it causes some problems. Specifically, IP pings for NSR frames fail at times.

- CSCdk46346

  If an encryption map is applied to a dialer interface, dialer pools are used, and a dial-up interface (for example, BRI) is used as the physical interface, then when that dial-up interface is unbound from the dialer it might cause a system reload or misalignment. A workaround is to not use dialer pools.

- CSCdk46537

  The length field in the MAC Management Message Header for the SYNC message is computed incorrectly. A workaround is to use a modem that has the Broadcom chipset. Because the SYNC message is a well known size, the Broadcom chipset can read the CMTS timestamp without looking at the length field.

- CSCdk46577

  On VIP interfaces where CEF is required to run encryption, a connection cannot be initiated from the VIP side. A workaround is to initiate the connection from a peer router (if the peer has a non-VIP interface). Encryption works properly in this case.

  On non-VIP interfaces with CEF enabled, encryption does not work properly, and packets are sent in the clear. CEF must be disabled for encryption to work.

  Note that this caveat affects only self-generated packets. In realworld environments, packets are usually forwarded to a router for encryption. In this situation, these packets are not affected by this caveat.

- CSCdk46820

  On a Cisco 2500 series router, you might fail to get CA certificates when enrolling a certificate with Entrust VPN.

- CSCdk46853

  In Release 11.2 P and 11.3 when Fast Ethernet subinterfaces are configured for encryption, if the encryption map is only applied to the main interface and the IP address is configured in the subinterface, the packets could be switched in the clear. In Release 12.0, enabling CEF could cause the packets to get dropped.

- CSCdk47147

  Cisco AS5200 and Cisco AS5300 access servers with MICA modems that are configured with the commands **async mode dedicated** and **async mode interactive** might fail with a bus error. On the Cisco AS5300, the failure is preceded with a "%ALIGN-1-FATAL" log message on the console. The cause seems to be a lot of PPP calls connecting and disconnecting.

- CSCdk47218

  If you configure output rate-limiting with distributed CEF enabled, on an interface that does not exist, you will cause a system restart.

- CSCdk48214

  Radius implementation for MS-CHAP does not comply with the latest specification from Microsoft.

- CSCdk48525

  POET output drops at low data rates with two PAs in VIP2. If you use a sub-rate POET interface together with a full-rate POET on the same VIP, VIP2 or VIP2-50, you will cause the full-rate POET to drop outbound packets. This occurs with an externally clocked sub-rate POET. There is no workaround, except to move the sub-rate POET or clock the sub-rate POET at 44.726 Mbps.

  Also see CSCdj86266 for a similar problem with HSSI interfaces.

- CSCdk49622

  After a Cisco 3600 series or Cisco 2600 series router is powered off and powered on, the ATM25 network module stops transmitting packets. Because a new image is loaded and an old image was previously on this platform, the problem will not be noted. This caveat appeared in Cisco IOS Releases 11.3(05.1)T and 12.0(00.2)T and was resolved by Releases11.3(6)T and 12.0(1.1)T.

- CSCdk49638

  Generic traffic shaping is not working on the Ethernet interface of a Cisco 2600 series router.

- CSCdk50099

  Packets larger than 1010 bytes fail to be transmitted on the BRI interface of a Cisco 7200 series router when WFQ is enabled (default queuing).

  Workaround: Enable FIFO queuing on the interface.

- CSCdk50394

  If an Ethernet or FDDI interface goes down for any reason other than administrative shutdown (for example, a cable is pulled), when the interface comes up, CEF adjacencies that existed before the down event do not come up. This results in dropping packets.

  Workaround: Clear the ARP table.

- CSCdk51089

  The router might reload when using the **default state-table** or **no state-table** commands. There is no workaround, besides avoiding using these commands. Also, confirm the existence of a particular state-table before deleting it.

- CSCdk51554

  Router displays an error message:

  ```
  42-1-NO_RING_DESCRIPTORS: No more ring descriptors available on 3 slot.
  ```

  Afterwards, ports on the VPM are no longer usable.

- CSCdk51931

  When trying to configure a multipoint ATM-DXI interface, the router only allows one **atm-dxi map** statement per VPI. For instance, if two ATM-DXI PVCs are defined on a multipoint interface (VPI/VCI 0/50 and 0/51), the router only allows one **atm-dxi map** command for VPI 0. The error message “Address already in map” appears when the second map command is entered.

- CSCdk53083

  Packets coming in on a tunnel interface from a Token Ring interface on a Cisco 2500 or 4000 platform are duplicated.

  Workaround: Disable fast switching on outgoing interface of unencapsulated packet.

- CSCdk53597

  Online insertion/removal (OIR) of a linecard caused the router to fail.

- CSCdk54004

  HSRP uses an incorrect MAC address to refresh the CAM on a switch or the MAC cache on a learning bridge. This can lead to loss of connectivity or possibly duplicate packets.

- CSCdk54291

  A router running lots of subinterfaces and distributed-CEF, might experience memory fragmentation problems due to excessive fibidb/fibhwidb download to linecards.

- CSCdk54652

  Connected host prefixes could remain in the linecard as invalid entries even when the interface is shutdown. This could happen if the interface down event was preceded by a full CEF download.

  Workaround: Issue the **clear cef linecard** command.

- CSCdk54726

  An LLC2 connection coming in from TR-ISL on a router and that should pass by way of DLSw can experience a setup failure. The **debug** command indicates “DLSw: failure - sap entry is not valid.”

  Workaround: Configure TR-ISL multiring on the FE subinterface although this is not normally required for SRB traffic.

- CSCdk55854

  The VIP fails when FEPA is configured for ISL and in the other bay a CT1 port adapter is installed. It is suspected that this problem can occur for FEPA+ISL along with any port adapter supporting subinterfaces.

  This problem did not occur for FEPA+ISL and serial port adapter.

- CSCdk56104

  While booting a router, the following traceback might appear:

  ```
  -Process= “CCVPM_VCSM”
  ```

  This will be followed by a traceback message, and some VPM ports become unusable.

- CSCdk57992

  In certain circumstances, when an encryption map is applied to an interface, removed, and subsequently reapplied, an RSP/VIP reloads.

- CSCdk58500

  If a ground-start link is initiated by the FXO port of a Cisco 3600 series router, the secondary dialtone returned by the connecting FXS port does not get passed through to a handset connected to the Cisco 3640 loop-start FXS port.

- CSCdk61362

  The use of an MBRI card in a Cisco 3600 series or Cisco 2600 series router with PPP encapsulation might cause packets to be dropped when CEF and L2F are enabled.

- CSCdk61689

  Turning on PVC OAM management on PA-A3 on the Cisco 7200 series router might cause the port adapter to crash if there is AAL5-NLPID PVC. The only workaround is to turn PVC OAM management off.

- CSCdk62934

  When the PA-A3 has physical layer errors at the 96th fifteen-minute status report interval, a memory overrun error occurs.

- CSCdk63661

  PA-A3 might stop receiving under stress with some CRC errors on VCs. Issuing the **clear interface** command can restore the service.

Novell IPX, XNS, and Apollo Domain

- CSCdj88812

  A router might report memory allocation failures caused by SAP general request storms, even though there is enough memory for the software image. If IPX Enhanced IGRP is configured, please also refer to CSCdk44590.

- CSCdk13645

  When using IPX Enhanced IGRP incremental SAP updates (RSUP), the server tables between two or more Enhanced IGRP neighbors might become inconsistent. Specifically, the problem might occur when as few as three dozen servers go away at the same time, while the routes to those servers remain in the routing table, and if there are multiple Enhanced IGRP neighbors or paths to a neighbor. The “down” flash update for some of the recently downed servers isn’t being sent out all interfaces, so some devices have the servers removed and others do not.

  Workaround: Clear the IPX Enhanced IGRP neighbors on the unit that shows these servers remaining in the table.

- CSCdk23276

  A Cisco 2500 router configured with the command **debug x25 events**, fails as it opens an X.25 VC for IPX, XNS, Vines, or DECnet.

- CSCdk42896

  IPXWAN does not work when a Cisco 4500 or Cisco 7200 series router is booted or reloaded with IPXWAN configured as the master of the IPXWAN link (its local IPXWAN node ID or IPX internal network number is larger than that of the router at the other end of the WAN link).

  You will see messages like these after IPXWAN debugging is enabled by issuing the command **debug ipx ipxwan**:

  ```
  00:06:45: IPXWAN: Rcv TIMER_REQ on Serial5/0/72000:0, NodeID 0, Seq 1
  00:06:45: IPXWAN: Rcv TIMER_REQ NodeID 7500 as SLAVE asking for unnumbered on Serial5/0
  00:07:05: IPXWAN: Rcv TIMER_REQ on Serial5/0/72000:0, NodeID 0, Seq 2
  00:07:05: IPXWAN: Rcv TIMER_REQ NodeID 7500 as SLAVE asking for unnumbered on Serial5/0h
  00:07:25: IPXWAN: Rcv TIMER_REQ on Serial5/0/72000:0, NodeID 0, Seq 0
  00:07:25: IPXWAN: Rcv TIMER_REQ NodeID 7500 as SLAVE asking for unnumbered on Serial5/0
  ```

  Workaround: After the router is rebooted, issue the following interface commands:

  – no ipx ipxwan

  – **ipx ipxwan** *parameters*.

  As an alternative, create a another pseudo IPXWAN interface which would allow IPXWAN to function after reloads; for example:

  ```
  !
  interface Loopback0
   no ip address
   no ip directed-broadcast
  !
  interface Tunnel0
   no ip address
   no ip directed-broadcast
   ipx ipxwan 0 unnumbered dtp-11
   tunnel source Loopback0
   tunnel destination 1.2.3.4
  !
  ```

- CSCdk44590

  The router gradually loses memory when running IPX Enhanced IGRP with **ipx sap-incremental** commands configured on its interface(s). The memory leak occurs when SAP general requests are received on the interfaces. By default, **ipx sap-incremental** is enabled on non-LAN interfaces which are configured for IPX Enhanced IGRP.

It is most easily seen by issuing the command **show proc mem**, and watching the growth of the "Holding" memory by the "IPX SAP In" process:

```
PID TTY Allocated  Freed   Holding   Getbufs  Retbufs Process
 44    0   14265416  201472    8360984     21924         0 IPX SAP In
```

Also, memory is being allocated to large number of IPX SAP PH, IPX NDB PH, and IPX USV processes, as shown by the command **show memory summary**.

Workaround: Remove IPX SAP incremental by issuing the command **no ipx sap-incremental eigrp** from the IPX interfaces.

Protocol Translation

- CSCdk51046

  A Cisco router running Cisco IOS Releases 11.3 or 12.0 might fail with bus error if the X.25 interface is congested and the PAD Virtual Circuit (VC) is cleared.

- CSCdk51892

  When using VTY-async interfaces, a new connection might be closed immediately after being accepted on the VTY.

TCP/IP Host-Mode Services

- CSCdk45442

  Issuing the command **privilege exec level** *level* **debug ip tcp packet** causes the router to fail if the commands **show running-config** or **write terminal** are issued.

Wide-Area Networking

- CSCdj35436

  A VIPs CPU load might go to 99% after an online insertion/removal (OIR) event. Only a system reload or microcode reload clears the problem.

- CSCdk26814

  Conditions under which the problem occurs: Any event that generates a media_hw_reset() such as changing an MTU size or clearing the ATM interface

  Signalling or ATM SVC applications such as LANE or static map refuse to create an SVC because they think it still exists. Clearing the ATM interface does not fix the problem.

  Workaround: Issue the commands **shutdown** followed by **no shutdown**, to clear all the state information at the signalling layer of the interface.

- CSCdk27818

  Voice over IP calls cause the router to reload if PPP Multilink is enabled on the BRI interface.

  Workaround: Force a UDP checksum on the dial peer, or remove the PPP Multilink.

- CSCdk28918

  MS Callback server functionality in Cisco access servers is not working with configurations involving async/ISDN interfaces configured with dialer profiles.

- CSCdk33096

  When the SERVICE messages are exchanged with the Routers for ISDN PRI interfaces, if the B-channels are transitioned from Out-of-service state to In-service state, the B-channel count does not get updated. This can prevent the router from dialing out or accepting incoming voice/modem calls. The remote callers get a fast busy signal.

- CSCdk36358

  On Cisco 3600 series routers, modems might repeatedly be unable to connect on the B-channel. The modems do not train up and the calls get disconnected.

- CSCdk37517

  DDR with **dialer dtr** does not reset DTR to a down state after an unsuccessful call attempt. Unsuccessful in this case means that DDR is triggered, DTR is raised, but the modem/TA attached to the serial port never connects, so that DCD does not come up.

  This can be verified by viewing **show dialer** to ensure that the dialer state is idle, and then **show interface serial x** to check the state of DTR.

- CSCdk39920

  When packets are bridged while a VC gets torn down, an incorrect VC value (zero) might be recorded in the bridge table entry. As a result, packets are dropped. This happens because the VC value gets set to zero before the subinterface gets brought down. The workaround is removing the invalid bridge entry by issuing the **clear bridge** command.

- CSCdk41028

  Fast port adapters (for example, FDDI, ATM, POSIP, and FE) on a VIP2 might see some performance degradation if the fast port adapter is on one VIP2 bay and other bay is empty.

- CSCdk41803

  A router using Cisco IOS Release 11.3(5.2) and later, with APPN and ATM configured, might experience software forced crashes with the following trace:

  ```
  crashdump
  process_suspend
  process_may_suspend
  cbus_atm_sendcmd
  cbus_atm_teardown_vc
  atm_remove_vc
  atmsig_remove_vc
  ```

- CSCdk41903

  Frame Relay SVCs might fail on multipoint subinterfaces.

- CSCdk43196

  A router leaks memory when both AAA and RADIUS/TACACS+ are configured on the router.

  Workaround: Issue the command **aaa accounting update periodic** *value* at startup time. Set *value* to a large number to avoid lots of periodic update accounting records.

- CSCdk45216

  The **multilink max-links** command does not work for L2F projected interfaces. This also applies for AAA user profiles which use the “max-links” TACACS+ attribute or Port-Limit and Ascend-Maximum-Channels RADIUS attributes.

- CSCdk46575

  Router might fail when the command **show dialer** is issued while calls are connecting and disconnecting.

- CSCdk46784

  Router might fail when running VPDN L2F sessions over ISDN.

- CSCdk46815

  LANE client might be dropped on a Cisco 7200 router. The workaround is to disable the SSCOP quick poll.

- CSCdk47523

  An attempt to switch an incoming call, when all outgoing channels are in use, causes a memory leak.

- CSCdk48335

  You cannot send break signal to a device connected to the asynchronous port on a Cisco 2511, through a PAD connection.

- CSCdk51529

  The router might reload when exiting a PAD connection. The problem first appeared in Cisco IOS interim Release 11.3(6.3).

- CSCdk52583

  Autoselect functions on VTY lines are not supposed to work, and should be disallowed.

- CSCdk55436

  A Cisco 1600 series router fails or reboots when Multilink PPP is negotiated on a link.

- CSCdk56005

  Under some circumstances when using X.25 switching, the router might reload.

  One example is when a call is switched to an XOT destination, which is then Cleared (when no Call Confirm was received).

- CSCdk62967

  The Cisco 2600 series routers with ISDN configurations—both Basic Rate Interface (BRI) and Primary Rate Interface (PRI)—can reload with a watchdog timeout when the ISDN interfaces are active/operational. This problem occurs only on Cisco 2600 series routers running Cisco IOS Release 11.3(6.2)T and later, Release 12.0(1) and Release 12.0(1)T. There is no workaround.

- CSCdk63455

  A router running translated X.25 to Virtual Async connections (PPP/IPX) might reload. This appears to be an infrequent occurrence.

- CSCdk64193

  Enabling IP multicast prevents LANE from populating multicast MAC addresses. As a result, it prevents IP routing protocols to work properly on LANE interfaces.

  Workaround: Disable IP multicast.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with release notes for Cisco IOS Release 12.0.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQ Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

© 1998-2000, Cisco Systems, Inc.
All rights reserved. Printed in USA.